Hospitality Security

Managing Security in Today's Hotel, Nightlife, Entertainment, and Tourism Environment

SECOND EDITION

Darrell Clifton

CRC Press
Taylor & Francis Group

HOSPITALITY SECURITY

Hospitality Security: Managing Security in Today's Hotel, Nightlife, Entertainment, and Tourism Environment, Second Edition provides experience-based, proven methods for preventing and resolving the challenges faced by today's hospitality security staff and leadership.

The lodging component of a hospitality environment creates challenges to the security professional by its complex set of assets and amenities—especially when combined with gaming environments. Whether the reader is establishing, or improving, a professional, proactive proprietary security force, or the manager of a boutique hotel, the practical methods described herein are applicable to everyone. Author Darrell Clifton takes the reader through a logical and methodical process to first evaluate what risks are inherent to hospitality environments, how to assess those risks through threat and vulnerability assessments and methods to mitigate, eliminate, or transfer them.

The book stresses the importance of prevention and investigation into the root causes of incidents as a tool for avoiding future undesirable events. This is especially important in that each registered guest brings with them their own unique set of circumstances, family values, problems, and social issues. The security function must operate to protect their individual rights, their right to privacy, and their desire to enjoy the facilities they are patronizing while contributing to the revenue stream. This must be balanced with the obligation, or duty, to provide reasonable care from foreseeable harm by the hotel to avoid incidents and litigation. Clifton, an experienced industry veteran, clearly establishes and identifies practical, reasonable, and cost-effective ways to accomplish this balancing of guest enjoyment with guest protection.

This new edition includes expanded content on premises liability, security force behavioral recognition, workplace violence, active shooter scenarios, evacuation planning, social media and guest reviews, and hotel scams. Additional coverage on nightclubs and bars has been added including four entirely new chapters on specialized security for events and venues, crime prevention through environmental design (CPTED), advances in technology, and industry trends for the gaming and hospitality sector.

Ideal for novices and veterans alike, *Hospitality Security, Second Edition* is an accessible, reader-friendly reference that enables security directors to evaluate what risks are inherent to hospitality environments, to analyze those risks through threat and vulnerability assessments, and to develop methods to mitigate or eliminate them—all the while keeping customers and personnel safe and improving the bottom line.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

HOSPITALITY SECURITY

Managing Security in Today's Hotel, Nightlife, Entertainment, and Tourism Environment

Second Edition

Darrell Clifton

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Cover Image: Top left, Maksym Fesenko/Shutterstock; top right, sixninepixels/Shutterstock; bottom left, dwphotos/Shutterstock; bottom center, one photo/Shutterstock; bottom right, diy13/Shutterstock.

Second edition published 2023
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

© 2023 Taylor & Francis Group, LLC

First edition published by CRC Press 2019

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

ISBN: 978-0-367-48005-9 (hbk)
ISBN: 978-0-367-48018-9 (pbk)
ISBN: 978-1-003-03764-4 (ebk)

DOI: 10.4324/b23281

Typeset in Palatino
by Newgen Publishing UK

Dedicated to the victims, survivors, families, and responders to the Las Vegas shooting on October 1st, 2017. May they rest in peace or find their peace.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

CONTENTS

Preface xxix
Prologue xxxi
About the Author xxxiii
What's with the Pineapple? xxxv

1 Risk Assessment 1

Premises Liability and the Risk Assessment 1
  External Risk Assessment 1
  Internal Risk Assessment 2
    Step 1—Divide the Property 3
    Step 2—List Threats 3
    Step 3—Severity 4
    Step 4—Probability 4
  Gathering Local Crime Data 4
  Police Data and Statistics 6
  Compiling Local Crime Data 7
  Gathering Proprietary Incident Data 8
  Gathering Market Incident Data 8
  Determining Likelihood 8
  Determining Risk 9
  Foreseeability 10
  Notice 11
  Managing Foreseeability 12
  Managing Risk 13
  The Living Document 13
  Talking Risk 14
  What Does Risk Have to Do with Security? 15
  Reacting to Risk 16
  Pre-emptive Risk Assessments 17
  Managing Threats 17
  Many of the Questions that Came from Media and Others after October 1 19

Reasonable Steps 19
Security Plan 20
Crime Prevention 21
The Crime Triangle 21
The Physical Protection System 21
What Is a Plan? 22
Accident/Incident Prevention 23
Decisions 24
Building the Plan 24
Outlining the Plan 26
Organization 28
Job Description 30
Policies and Procedures 31
Overall Property 32
Specific Areas 33
Incident Action Plan 33
Summary 34

2 Policies and Procedures 37

Hierarchy of Rules 37
Regulations, Standards, and Other Legal Mumbo Jumbo 37
Elements 40
Codes 42
Standards 43
Guidelines 43
Best Practices 43
Company Policies 44
Types of Manuals 44
Policy vs. Procedure 44
Company Manual 45
Security Manual 46
Training Manual 47
Building Your Manual 47
Foreword 47
Department Policies—Section 1 48
Organization—Section 2 48
Employee Policies—Section 3 49
Posts/Patrol Areas—Section 4 49

- Systems/Procedures—Section 5 50
- Crimes and House Policies—Section 6 50
  - Arrests 50
- Emergency Procedures—Section 7 50
- Incident Response—Section 8 51
- Documentation—Section 9 51

Writing the Manual 51
- Other Sources 52
- Delegation 53
- Compiling 54
- Updates 54
- Summary 54

Emergency Manual 55
- Hazards and Threats 55
- Starting the Emergency Manual 56
- Testing the Manual 56

Incident Action Plan 56

3 Training 59

Making the Case for Training 59
- Ability 59
- Consistency 60
- Liability 61

Funding Training 62
- Guest Safety 62
- Liability 63

Training Culture 63
- Training Manager 64
- Unique Classes 64
- Include Everyone in the Process 64
- Continue the Training from Day One until the End of Time 65

Quality In Is Quality Out 65

Consistency 66

Training Program 67
- Training Components 67
- Classroom 67
- Training Objective 68
- Basic Laws 69

    Laws of Arrest 69
    Search and Seizure 70
    Use of Force 70
    Use of Force (More Stories Later) 73
    Company Policies 75
    Report Writing 75
    Emergency Procedures 75
    Guest Service 76
Field Training 77
    Task List 78
    Evaluations 79
In-Service Training 79
Defensive Tactics 81
Documentation 83

4 Staffing 85

Guards or Officers? 85
Hiring 86
    Recruitment 86
        Job Posting 86
        The Screener 87
        Qualifications 87
        Starting Wage 88
        Loosen Up 88
    Application Process 89
    Interview 90
        Standard Questions 91
        The Questions 91
        Second Interview 92
        Group Interview 92
    Background 92
        Drug Testing 94
    Before Hiring 94
    Orientation 95
Deployment 96
    Schedules 97
    Minimum Staffing 99

Wage Structure 99
  Survey 99
    Base Wage 99
    Raises 100
    Training 100
    Experience 100
    Benefits 100
    Reputation 100
  Officer Development Program 101
Contract Security 102
Leadership 105
  The Hierarchy 105
  Creating Managers 106
  Responsibility 106
  Supervision 106
  Training and Coaching 107
  Delegation 107
  Managing Managers 108
Maintaining Morale 110
  Empowerment 111
  Other Morale Boosters 112
  Image 112
  Guards 113
  Recognition 113
  Proper Training and Equipment 113
Patrol 114
  Overall Property 114
  Physical Protection System 114
    People 114
    Deployment 116
    Work Force 117

5 Patrol 119

Basics 119
  Prevention 119
    My Perception of the Recent History of Policing 120
    A Tale of Two Cities 120

  Preventive Patrol 121
  Posts 123
  Post Types 123
  Post Orders 125
  Elevators 125
Hotel Patrol 126
  Combining Layers 128
Summary 129
  VIP Protection 129
  Dispatch 131
    Communication 132
    System Monitoring 132
    Documentation 132
  Patrol Procedures 132
  Safety 133
  Parking 134
  Headcounts 134
  Purse Advisories 134
  Loiterers 135
  Eye Contact 135
  Greeting 135
  Patrol Duties 135
  Room Entry 135
  Housekeeping 137
  Marijuana 137
  Service Animals 138
  Wheelchairs or Other Mobility Devices 138
  Parties in a Room 138
  Underage Drinkers 139
  Domestic Fights 139
  Cooking and Other Unsafe Practices 140
  Door Ajar 140
  Welfare Check 141
  Privacy 142
  Unknown Guest 142
  Room Inventories 143
  Weapons 144
  Room Thefts 144

- Violent Crimes 145
- Restrooms 145
- The Lobby 147
- Lost and Found 147
  - Administration 147
- Tracking 148
  - Found Objects 148
  - Valuables and Cash 148
  - Storage 148
  - Do the Math 149
  - Disposition of Items 149

Security Measures 149

- Search Stations 149
- Arrests 150
- Refuse Service 151
- Trespassing 151
  - Last Resort 152
  - Procedures 152
- Video Patrol 153
- Camera Placement 154

Special Training 156

- Bike Patrol 156
- Escalators 158
- Spas and Pools 160
  - Lifeguards 160
  - Pool Rules 160
  - Safety Equipment 161
  - Hot Tubs 161
  - Spa Treatments 161
  - Chemical Hazards 162
  - Pool Parties (Wet Clubs) 162
  - Theft 162
- Valet 163
  - Employee Theft 164
  - Guest Accidents and Injuries 164
  - Vehicle Damage 164

- Conventions, Meetings, and Banquets 164
  - Event Type 166
  - Specific Group 166
  - Number of People and Demographics 166
  - Alcohol 166
  - BYOB 166
  - Music 167
  - Politics 167
  - Admission 167
  - Merchandise 167
  - Security 167
  - Dress and Prohibited Items 168
  - Age 168
  - Crowd Management 168
  - Minor Events 168
  - Security Plan 168
  - Special Event Permits 169
  - Outdoor Events 169
- Parking 170
  - Cleanliness 170
  - Lighting 171
  - Access Control 171
  - Security Patrol 172
  - Parking Enforcement 172
- Casino Security 172
  - Casino Controls 173
  - Regulation Hierarchy 175
  - Casino Patrol 175
  - Detention 176
  - Deployment 177
  - Innovation 177
- Medical 178

6 Physical Security and Crime Prevention Through Environmental Design (CPTED) 179

- CPTED 180
  - Crime Prevention Through Environmental Design, by Russell Kolins 181

- Exterior Physical Security 182
  - Landscaping 183
  - Lighting 185
  - Put It All Together 187
- Physical Barriers 187
- Walls and Fences 189
- Conclusion 189

7 Emergency and Incident Response 191

- Major Emergencies 191
  - Fire Alarm 192
    - Directional Signage 192
    - Means of Egress 193
    - Doors 193
    - Alarm Function 193
    - False Alarms 194
    - Bottom Line 194
  - Fire 194
  - Active Shooter 195
    - Response 197
    - Security Response 199
    - Objective 199
    - Physical Response 199
    - Police Notification 199
    - General Procedures 200
    - Additional Details 200
  - Panic Alarm 200
  - Bomb Threat 201
  - Medical 202
  - Suicidal 203
  - Lost Child 203
  - Weather—Blizzards, Hurricanes, Rain/Flood, Winds 204
  - Earthquake 205
  - Power Failure 205
  - Indoor Contaminant Release 205
  - Outside Chemical Release 206

Secondary Effects 206
  October 1, Las Vegas Mass Casualty Incident 206
  Recovery 208
  Mutual Aid 209
Incident Response 209
  Medical Incidents 210
  Domestic Fights 210
  Suspicious Person 211
  Trespass 211
  Room Losses 213
    Value of Item 214
  Crimes in Rooms 214
  Proprietary Loss/Damage 214
  Room Disturbance 215
  Bed Bugs 215
  Major Incidents 216
  Guest-Room Attendants 217

8 Investigations 219

Preliminary Investigations 219
  Initial Response 220
    Preparation 220
    Response 220
  Starting the Investigation 221
    Photos 221
  Witnesses 222
    Interview 222
  Evidence 222
  Drugs and Contraband 223
Report Writing 223
  Format 224
  Narrative 224
  Corrections 225
  Attachments 226
  Next Steps 226
  Retention 226
  Report Writing Software 227

Investigations 227
  Report Follow-Up 228
  Personnel Investigations 229
  Interview 231
  Victim 231
  Witnesses 232
  Non-witnesses 232
  Character Witness 232
  Suspect Employee 232
  Post-interview Conference 233
  Interrogation 234
  Resignation versus Termination 234
  Cooperation 235
  Unions 235
  Translators 236
  Burden of Proof 236
  Criminal Investigation 236
  Private versus Public 237
  Restitution 237
Workers' Compensation Investigation 238
Guest Claims 239
  Triggers 239
  Statements 239
  Witnesses 239
Analysis 240
  Metrics 240
  Data Sources 240
  More Data Is Better 241
  Analyzing the Data 241
  Slip and Falls 243
Crime Analysis 243
  Location 244
  Crime Type 244
  Time 244
  Suspect 244
  Other Sorts 245
  Crime Triangle 245
    Suspect 245

        Victim 246
        Location 246
    Off-Property Incidents 246
    Reacting to the Data 247
Special Operations 247
    Undercover Operations 247
    Outside Agencies 248
    Private Outside Agencies 248
    In-House Operations 248
        Integrity Checks 248
        The Preliminaries 249
        The Setup 250
        Now Some Warnings 251
        The Sting 251
        More Warnings 251
    Covert Cameras 252
    Bag Checks 253
Drug Testing 254
    Random 254
        Random Testing 255
    Post-accident 255
    Cause Testing 256
Abandoned Luggage 256
    Risk Assessment 256
    Back Track 256
    Internal Procedures 257
    Official Response 257
Internal Crime 257
    Employee Crime Stats 258
        Internal Audit 258
    Security Audits 258
    Types of Audits 259
    Performing Audits 259
    Fraud Detection 260
Accounting 260
    Payroll Scams 260
    Collusion 261

  - Credit Card Fraud 261
  - Identity Theft 262
  - Charge-Offs 262
  - Fake Vendors 262
- Cashiers 263
  - Voids 263
  - Returns 263
  - Coupon 263
- Restaurants 263
- Receiving 264
  - Outgoing Theft 264
  - Receiving Theft 264
  - False Orders and Return Thefts 265
  - Lost Merchandise 265
- Housekeeping 265
- Security 265
- Background Checks 266

9 Executive Skills 269

- Finding Your Place 269
  - Cooperation and Collaboration 270
  - Executive Meetings 271
- Communication 272
  - The Boss 272
  - Your Staff 273
    - Maintaining Morale 274
- Your Peers 275
  - Networking 275
  - Government Meetings 276
  - Associations 276
  - Local Trade Groups 276
  - Nonprofit Groups 276
  - Public/Private Groups 276
  - Online 277
  - Regional Training 277
  - Regional Communication 277
  - Mutual Aid 277

- Written Agreement 278
- Sharing of Resources 278
- Regional Disaster Planning 279

Personal Growth 280

- Your Work Ethic 280
- Stress 280
- Time Management 281
  - Delegation 281
  - Visibility 281
- Respect 282
- Attitude 282
- Tactical Planning 283

Budgeting 284

- Basics 284
- What Is It? 284
- Prior Year 284
- Process 284
- Full-Time Equivalent 285
- Wages 285
- Recurring Expenses 285
- Overtime 285
- Benefits 286
- Budget Submission 286
- Your Budget 286
- Capital Expenses 287
- Life Safety 287
- Saving Labor 288
- Security Envy 289
- The Pitch 291
- Security Revenue 291
- Restitution 292
- Parking 292
- Special Events 292
- Lost and Found 293
- Back-Charging 293

Justifying Security 293

- Crime Rates 293
- Internal Crime 294

- Guest Comfort Level 294
- Terrorism 294
- Making Those Cuts 294
- Creative Scheduling 294
- Briefing 295
- Supervisors 295
- Spending 295
- Procedural Changes 295
- Patrol Areas 296
- Arrests/Reports 296

10 Nightclubs, Restaurants, and Bars 297

- Alcoholic Beverages 297
  - Alcohol 298
  - Guest Service 300
- Training 301
  - Training Topics 301
  - Appearance 301
  - Shared Labor 302
- House Policies 303
  - Age Requirements 303
  - Identification 304
  - Crowd Manager 306
  - VIPs and Known Persons 307
  - Tips 307
  - Bottle Service 308
  - Prohibited Activity 309
  - Dress Code 309
  - Prohibited Items 310
  - Searches 311
  - Weapons 312
  - Drugs 312
  - Date Drugs 314
- Violence 314
  - Pre-violence 315
  - Taking Action 315
  - Ejections 315
  - Occupancy 316

- Staffing Ratios 316
- Restrooms 317
- Emergency Exits 317
- Re-entry 317
- Hand Stamps 318
- ID Scanners 318
- Closing Duties 319

Posts 319
- Line Control 319
- Door Host 320
- Floor Person 321

Situations and Procedures 322
- Violence 324
- Ejections 325
- Intoxicated Persons 325
- Trespasses 325

Use of Force 326
- Policy 326

Emergency Procedures 328
- Person Down 328
- Fight (Two or More Persons) 329
- Ejections 331
- Fire Alarm—Sirens and Strobes 332
- Smoke or Fire 332
- Power Failure 332
- Earthquake 332
- Hurricane/Blizzard/Tornado 332
- Active Shooter/Shots Fired 333

Restaurants 333
- Slips, Trips, and Falls 333
- Food Poisoning 334
- Allergies 334
- Now the Financial Stuff 334
  - Walk-Out 334
  - Credit Cards 335

Bars 336
- Over-Pouring 336
- Over-Serving 337

  Over-Charging 337
    By Russell Kolins 338
    CPTED Concepts 338
    CPTED Basic Principles 338
    Natural Surveillance 339
    Access Management 339
    Territoriality 339
    Facility Maintenance 339
    Order Maintenance 340
    Activity Support 340
    It Starts with a Plan 340
    CPTED Checklist for Venues that Serve Alcohol—Bar Area 347
    Internal Layout 347
    Crowding 348
    Lighting 348
    Outdoor Drinking Areas 348
    CCTV 348
    Entrances and Exits 349
    Staff 349
Retail 349
  Policies 349
  Shoplifting 350
  Catching Shoplifters 350
  Arrests 351
  Preventing Shoplifting 352
  Retail Staff Training 352
  Store Layout 353
  Cameras and Mirrors 353
  Antitheft Devices 353
  Organized Retail Crime (ORC) 354
  Credit Cards 354

11 Employee Awareness 357

Culture Change 359
  Ownership 361
  Communication 361

    Awareness 362
  Security Awareness 363
    Housekeeping 363
      Drugs and Paraphernalia 363
      Parties 364
      Weapons 365
    Prostitution 365
    Safety Hazards 365
    Criminal Activity 366
  Front Desk 367
    Identity Theft 367
    Key Theft/Room Entry 367
    Night Auditor 368
    Vertical Security 368
  Hotel Operator 368
    Credit Card 369
    Vandalism 369
    Long Distance Call 369
    Purchasing Scam 370
  Behavioral Recognition 370
    Step One—Objective 371
    Step Two—Observe 371
    Step Three—Second Look 371
    Step Four—Challenge 372
  Social Engineering 374
    Front Desk 374
  Workplace Violence 377
    Type I—Criminal Acts 377
    Type II—Customer/Client/Patient Violence 377
    Type III—Worker-on-Worker Violence 378
    Type IV—Violence Stemming from a Personal Relationship 378
    History 378
    Conclusions 379
    Anger 379
  Workplace Violence Policy 380
    Developing the Program 380
    Related Policies 382
    Training Program 382

- Threat Management Team (TMT) 383
- Domestic Violence 383
- Conclusion 384

Valet Parking 384
- Video Cameras 385
- Reducing Obstacles 385
- Back It In 385
- Background Check 385
- Height 386
- The Ticket 386
- Clearance 386
- Theft Claims 386
- Drunk Drivers 386
- Porte-cochère 387
- Concourse 387
- The Point 387
- Podium 387
- Office 387
- Keys 387

Virus 388
- Virus Overview 389
- Airborne 389
- Ingested Poisons 390
- Contact Poisons 390
- Prevention 390
- Mitigation 391
- Norovirus 391
- Preventing Norovirus 392
- Water Supply 392

Prohibited Items 393
- Microwaves and Other Appliances 393
- Coolers 394
- Pizza Coupons 394

Trafficking/Prostitution 394
- End-User 397
- Pimp 397
- Solutions 399
- Front Desk Clerks 399

  Guest-Room Attendants 400
  Valet, Bell, and Concierge 400
  Online Enticement 402
  Child Sex Trafficking 402
  Child Pornography 402
  Prostitution Glossary (Caution: Explicit Language) 403
Drug Use 404
  Marijuana 404
  Parties 405
  Unplanned Parties 406
  Sales Groups 406
  Squatters 408
  Sub-Letting 409
Safety 410
  Objective 410
  Culture of Safety 410
  Safety Value 411
  Executive Team 411
  Coordinator 412
  Accountability 412
  Participation 413
  Efficiency 414
  Branding 414
  Program 415
  Compliance 415
  Awareness 416
  Safety Committee 416
  Departmental Inspections 417
  Training 417
  Communication 418
  Safety Newsletter 418
  Safety Wall 418
  Safety Suggestions 418
  Insurance Company 419
  Workers' Comp 419
  Accidents 419
  Documentation 420
  Risk Management 420

  Restroom Logs 421
  Safety Sweeps 421
  Spill Stations 421
  Escalator Shutdown 421

12 Technology 423

Guest Surveys 423
  Guest Satisfaction 424
  Employee Development 424
  Fresh Ideas 425
  Liability 425
Fire Alarms 425
  Sensors 425
  Panel 425
  Communicator 426
  Types of Alarms 426
  Fire Sprinklers 426
Metal Detectors 426
  Concerts 427
  Policy 427
  Placement 428
  Settings 428
  Bottles/Liquor 428
  Searches 428
  Wands 429
  Smoking; Re-Entry; In and Out 429
  Cell Phones 430
  Manpower 430
Crowd Management 430
  Planning 431
  Communication 432
  Direction 432
Gun Shot Detection 433
Artificial Intelligence 433
Anti-Terrorism 434
X-Ray Luggage 435
Bomb Dogs 435
Data Security 436

- Data Investigations 438
- Employee Duress 438
- Tour Tracking 439
- Employee Lockers 440
  - Issuance 440
- Key Control 440
- Video 440
- Cameras 440
  - Analog and Digital 441
    - Digital 441
    - Lens Types 442
    - Compression 442
    - Speed 443
    - Analytics 444
  - Applications 444
  - Facial Recognition 444
  - Analytics in Real Life 445
  - Deterrence 445
  - Detection 446
  - Elevator Camera 446
  - Investigation 446
- Guest-Room Locks 447
  - Elevator Keys 449
- Radios 449
- Report Writing Software 450
- License Plate Recognition 450
- Robots 451
- Armed Security 451
  - Off-Duty Police 452
  - Contract Security 453
  - Proprietary Security 454
  - Hiring 456
  - Training 456
  - Tasers 458
  - Weapons Policies 458
  - Conclusion 460

Index 461

PREFACE

I dedicated this book to the victims of the Route 91 Harvest Festival Shooting on October 1st, 2017. May they rest in peace or find their peace.

That shooting, the deadliest in US history, had an impact on so many of us. To me, it was like 9/11 in its magnitude and carnage, yet this one seemed worse somehow. I know that way more souls perished in 2001, and maybe I am affected by the proximity of this attack or the industry the attacker exploited. While 9/11 saddened me and angered me, this one went farther. For one, it scared the crap out of me, which I will explain shortly. This one seemed personal, and we still struggle to know why he did it. On a professional level, motive has absolutely nothing to do with the work of prevention. But there are certain givens that we humans afford each other and he broke all of them. There is a trust we have in even the most despicable people that we will not have again.

Everyone has a story of how disasters or horrible events affected them personally. Though I find this a bit narcissistic, I want to give you my perspective, as we will use it later. On Sunday night, September 30, I was in Las Vegas, in my hotel room about a mile from the festival. Many of us had gathered for a gaming conference and I was teaching an active shooter class the next day. At one point I began to hear sirens. This went on for several minutes and I finally turned on my trusty scanner app. It seemed as though there was a shooter inside the festival, and the confusion was apparent. Immediately, dispatch began reporting more shooters up and down the strip. These casinos seemed too far away to be catching "collateral" from the original. In fact, I thought that Las Vegas was experiencing a coordinated attack that had been anticipated since 9/11. It turned out that victims from the festival were walking or being driven as far away as three miles up the strip. When they walked in the doors of each casino and said they had been shot, the assumption was that the shooter was out front. A clever police commander, who had been monitoring all of the "Active shooter" calls at other casinos, finally told Dispatch to contact security at those locations and to stop sending resources unnecessarily. I felt helpless without a car, so I listened most of the night. I learned a great deal from the scanner and followed it up with discussion the next morning with all my classmates who were also feeling helpless.

I have several more references to October 1 throughout the book. I hope you get something out of it. If you are not familiar with it, I encourage you to search online for "LVMPD Criminal Investigative Report of the 1 October Mass Casualty Shooting." This 187-page report is complete with photos and diagrams and leaves nothing out. There is often a similar report after all sorts of events. These are free and worth the read so you can prepare your properties.

This brings me to a couple of warnings before you dive in. First, every story related in this book is true. It either happened to me, a colleague, or I got it from a reputable news source. Second, I do not use citations or footnotes, which is why I leave out sources and names. I do try to provide enough information that you can search the incident if you want. Third, I use the male pronoun to denote both genders (mostly). I swear I am not a misogynist—it is simply the way we were taught in the old days. Not sure if it still is. Finally, I will observe and admit that security directors are arrogant, especially my brothers and sisters in the casino business. It is hard to take advice, suggestions, or recommendations from someone else. I have two things to say about that. One is that you can use anything in this book without giving me any credit. Say it is your own idea and I will not tell anyone. (But if you cite the book, you might get a little more traction behind you.) Second, if a friend or boss gave you this book to get some pointers, please give it a shot. It might support some initiatives you wanted to try anyway.

Most of the examples and stories herein are related to big hotels and big proprietary security departments. But I really wanted this book to appeal to the bar owner, hotel manager, and those with small staffs or no security personnel. I urge you, if you fit in a category like that, to take away the lesson and not the size. Just about everything can be scaled down and applied to all of these venues.

PROLOGUE

The most significant event to impact our industry—maybe every industry—was the October 1 shooting in Las Vegas, Nevada. That event forever changed the way security plans, implements, operates,—heck, it just changed everything. That day changed beliefs and assumptions that I held for 30 years. As Security professionals, we all want to make sense of these types of tragedies so that we can learn from them, prevent them, and help others prepare for them. Here are some thoughts of mine on this incident that have helped me cope with it. Maybe they will help you as well.

Motive—We, as a culture, want to know a motive whenever a murder occurs. (At least that is what the media tells us we want.) Everyone, even the Sheriff and the FBI say they do not know the motive. Well, the motive is anger, in my opinion. It is always anger. Every killer is motivated by anger. If the subject of the anger is not rational or known to us, it is because a mass murderer, by definition, is insane. Crazy. Mentally ill. If their anger is not directed at someone you know, it is directed at whatever voices or fantasies they have in their head. We cannot possibly know what those ideations were because he is dead. So, if someone says it is too bad we did not know his motive, just tell them he was angry at the voices in his head.

Blame—We also live in a society that likes to point fingers. We cannot close anything until we have a fall guy—someone who can be held responsible. While I respect everyone's right to use the legal system to hold others accountable for their negligence, let's not lose sight of the fact that one person did this horrible thing and no amount of foresight, preparedness, expertise, or money can prevent someone from doing bad things. Of course we will learn from it and make every effort to prevent it from happening again but we all have ideas in our head of how we could do that and the only thing stopping us is our morals and our sanity.

Technology—The questions I was asked on October 2 by several media organizations were all about technology. Should hotels have metal detectors? Do you think hotels will install bullet-proof glass? What will security spending look like from now on? I was dismayed to hear our media going in this direction before the bodies had even been identified. I am a big supporter and buyer of new technology and it is necessary in a constantly advancing society but come on!

This book will look at the Physical Protection System that is made up of Humans—personnel, staff, guests, you, and me; Policies and Procedures—Laws, rules, regulations, signs; and Technology—Gadgets, things, alarms, doors, CPTED, and so on. So, while technology may count for a third or so of measures that may be taken to prevent such an incident, we cannot leave out the other two for a rounded approach.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

ABOUT THE AUTHOR

Darrell Clifton is a Board Certified Security Professional with 30 years of operational experience. Beginning his career as a security officer, he worked his way to director and beyond. He also cross-trained in all the departments of the hotel/casino, rounding out his expertise in all areas of the hospitality industry. After three decades managing security departments, he now provides comprehensive training for frontline and management on topics like active shooter, workplace violence, human trafficking, and much more. Having been awarded Security's Most Influential Person, Darrell also consults as a subject matter expert, providing expert testimony in all matters involving security and/or hospitality.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

WHAT'S WITH THE PINEAPPLE?

The pineapple has been a symbol of hospitality since the "New World" was being explored a few centuries ago. When ships came in from Europe to the Caribbean and other tropical places, they were presented with gifts of native fruits. These baskets were always crowned with the pineapple. The explorers were so impressed with the regal fruit that they took them back to their kings and queens who, of course, demanded more. The locals started the tradition of giving fruit baskets and of displaying a pineapple to let guests know they were always welcome.

Now when you see a pineapple in a hotel or the fruit carvings on cruise ships and elsewhere, you will know you are welcome.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

1

Risk Assessment

PREMISES LIABILITY AND THE RISK ASSESSMENT

I start this second edition, like the first, with Risk Assessment. This is a dry topic, but a necessary one so I will try to make it as quick as I can. If you are like me, you entered this field from the operations side, walking around in a uniform, greeting guests and taking care of business. Nothing in your long-term career plans included doing assessments (or budgets—just wait for that chapter), but I hope to gently get your buy-in on this process. Follow along and give me a chance here.

By the way, before I proceed further, I will admit there are many books written on this topic by people smarter than me with better vocabularies—well, more sophisticated word uses anyway. You might consider mine more operational and less academic. My methods are simpler and more common here in the real world.

Did you know you are already doing risk assessments? You do it when you drive, when you meet a stranger—or hire one, and even when you spend the company's money. I will explain that one in Budgeting. Whether your property is in design phase, recently completed, or an established destination facility, a Formal Risk Assessment needs to be completed. A properly researched and considered Risk Assessment will not only help management plan protective measures, but it will also provide a legal defense for those measures.

Many hotels have been in operation for years and have never completed a formal Risk Assessment. Frankly, I worked for one of those companies and the business ran just fine. I think they preferred to react to situations rather than prevent them. Those huge companies can afford that, but the rest of us are directed by our own wallet and the rules of the insurance company. Informal Risk Assessments are performed constantly by security professionals, engineers, and risk managers. Formal or informal, the process is largely the same. Your first decision is whether you should do this process yourself or hire a professional.

External Risk Assessment

An outside consultant can add some integrity to your Risk Assessment. Many people, including me, make a good living sharing their experience, their knowledge of other

DOI: 10.4324/9781003037644-1

properties, best practices, and reputation. These professionals will lend some credibility to the finished product. They are also likely to think of some things that you could not—not because they are smarter, but because they have been around a few blocks while you have been working for a living. Trust me, I know the arrogance of security directors, having been one, and it is hard for them to let someone in. Your company already uses outsiders for interior design, most of the security framework, and even accounting and marketing. Consider the external assessment.

There are some software programs that perform these assessments. The variables are so many that the program ends up being inadequate or needs customizing to the extent that it turns into a glorified reporting tool. However, if you are on your own, it may help you crunch numbers so you can formulate the research and presentation. Insurance professionals and meteorologists use something like this to make "predictions" in their worlds. The only way I see Risk Assessment software as an advantage is if you have multiple locations.

Internal Risk Assessment

An Internal Risk Assessment is one that is done by you—or a team within your organization. The advantages of this method are that you know your business, its history, and trends in the region (hopefully). If you take this on yourself, you will undoubtedly learn a great deal. Perhaps you do both—do it in partnership with a professional or have her review your work. Unless you just do not feel comfortable nor have the time.

A Risk Assessment is quite simply a calculation of severity and probability. Oh my gosh, I just used three big words in one sentence. (I try not to do that because it frankly puts me to sleep when I read.) A Risk Assessment is quite simply finding how likely something is and comparing it with how bad it would be if it happened. There.

Don't let the math scare you. Security professionals perform these assessments on a regular basis—and they do so in their head. Each time a security officer approaches someone in the hotel, a mental Risk Assessment is being performed: He evaluates the likelihood of the person being a danger and then he decides the worst thing that could happen. The data he compiles in that one second are: appearance, actions, time of day, location, lighting, other persons around, and many other factors. The immediate results of that mental calculation are used to determine the officer's stance, demeanor, reaction, and level of readiness. For example, a petite, elderly, intoxicated woman trying to get her room key to work generally would not pose the same threat or prompt the same response as a tall, muscular, younger man. That is a simple Risk Assessment. In his head, he calculated the probability of that person being a threat (attacking him) and he counted the severity of that threat (big guy versus little old lady) and made an instant decision to prepare himself.

The Risk Assessment process takes this simple calculation, expands it for a variety of threats, under many conditions, and formalizes it so that a security plan can be developed and documented for use later in justification. So, why do we need to go through all of this if we can do it in our heads? To protect our assets in court. I will explain toward the end of this chapter, but first, the assessment. This process can be divided into five steps. First, we will divide the property into sections. Then we will list all the possible threats and hazards for each area. Next, we will compile some historical facts to determine probability.

After that, severity will be figured into the process. Finally, we will work with the resulting values to determine risk.

Step 1—Divide the Property

The only difference in our assessment and the ones made on the fly every day, is that this one will be in writing and it will cover all threats. Step 1 is to categorize the property into areas. Each area is like its own business with its own particular threats and risks, so it will be simpler to work with them separately. Do this by physical location, department, or revenue center—whatever makes sense to you. We will do a separate Risk Assessment for each of these areas, such as front desk, nightclub, guest rooms, and retail store. Some threats and hazards are to the entire property—such as floods and hurricanes—although the likelihood and severity will depend on your location. These are addressed in Chapter 7. We will use "Guest Rooms" as an example of one of our sections for the remaining steps (see Table 1.1).

Step 2—List Threats

Step 2 is to list the threats for each area. Consider every threat, no matter how remote its possibility. For our purposes, threats are crimes, natural hazards, and accidents. In Table 1.2, some examples of threats are robbery, domestic violence, property theft, assault

Table 1.1 Risk Assessment Example (Guest Rooms)

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious 1 = Least Serious	**10 = Most Likely 1 = Least Likely**	**Severity × Probability**

Table 1.2 Listing Possible Threats

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious 1 = Least Serious	**10 = Most Likely 1 = Least Likely**	**Severity × Probability**
Robbery			
Domestic violence			
Property theft			
Assault on employee			
Noise complaint			
Fire			

on employee, noise complaint, and fire. These are not all of the threats that can occur in a guest room, there may be many more.

Step 3—Severity

Severity is completely subjective. The numbers we come up with are for ranking only. We are going to fabricate these numbers based on our own common sense or opinions. Different persons may evaluate severity a bit differently, but even that will not matter for this exercise. Even though opinions vary, most people will rate incidents relatively the same. Death is more serious to everyone than vandalism, so the values are not as important as their ranking with the other threats.

For the purpose of this Risk Assessment, Severity is a rating of 1 to 10 on how bad the event would damage the assets or persons. Death would be a 10 and excessive noise in a hotel room is likely a 2. In Table 1.3, I have assigned values to each of the threats based on my opinion of a sample hotel. I made "Fire" the most serious with a rating of 9 because it can do the most damage and disrupt business most severely. I rated "Domestic Violence" and "Noise Complaint" as least severe with 2 each. Both of these types of incidents cause a minor disruption to a few other guests and it is unlikely the hotel would suffer any loss from either. Your ratings may be different and that is fine as long as you can justify them.

Step 4—Probability

In order to determine probability, we need to do some research. Although our severity numbers in the table were subjective, the probability numbers better have some backing, or you will look ignorant in a deposition and to your boss. Backing comes in the form of historical crime data.

Gathering Local Crime Data

Before risk can be assessed, some incidents need to be reviewed. First is historical "neighborhood" criminal activity. Criminal activity would include just about every type of activity that could happen at the hotel. In our risk assessment, we will compare like crimes, so gather everything even if it does not seem relevant.

Table 1.3 Determining the Severity of Threats

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious 1 = Least Serious	**10 = Most Likely 1 = Least Likely**	**Severity × Probability**
Robbery	8		
Domestic violence	2		
Property theft	5		
Assault on employee	8		
Noise complaint	2		
Fire	9		

There are several possible sources for local crime activity, the most likely of which is the local police department. Many police departments provide regional crime data and calls for service through public source Internet sites or apps. Others provide it by less technically advanced means like paper reports or spreadsheets available from the police station or city hall. Most large cities like Los Angeles, Las Vegas, and Chicago have easy-to-navigate Web sites that provide crime data that can be filtered and sorted. Many smaller cities provide this service as well. The easy way to find out is to do a search for your city name and "crime data."

There are other privately owned, but free, Web sites that provide this service for most cities using public information. Try searching "crime data by city" or "crime data by zip code." Of course, a few crime analysis companies provide this information for a fee. The price may include the Risk Analysis that is being explained here and other valuable information from other sources combined into one professional presentation. Consider these services to save time.

If the local law enforcement agency does not provide this data in an electronic form, it may be necessary to query them personally. This is public information, but there may be a fee associated with compiling the information or copying files.

Other sources for historical crime data are the Business Improvement District, Business Owners' Association, or Chamber of Commerce. The hotel may already belong to such a group, which generally has this information compiled or can easily access it through its law enforcement liaisons.

Many security departments will task someone with keeping this neighborhood crime activity documented and categorized (see Chapter 8). There are other investigative reasons for doing this, but for the Risk Assessment, it fulfills the data-gathering requirement. This is an easy process to set up and the events can be taken from a police blotter in the news, personal contacts at the police department, or regular phone calls to the report desk.

> I used to run a hotel team in an urban environment (downtown) that had the only armed security in the northern part of the state. I had my investigator track every violent crime in our area and plot it on a map—including those crimes on our property. I had this ready in case our need for guns was threatened. The data, though I never used it, was to my expectation: less violence on the property than around it. This turned out to be kind of a backward risk assessment because the security plan was justified based on incidents that had already occurred.

When gathering crime data, it is important to establish the radius or area from which the data are derived. This depends entirely on the location of the property. If the property is in a downtown urban setting, a few blocks square would probably do it. Rural areas may require much larger area to get enough data. Getting enough data is the best rule of thumb for determining sample sizes. You may be familiar with Gerrymandering. This is a process of creating precinct boundaries for voting and political representation. One party generally accuses the area of drawing the lines in such a way as to get more like-minded persons in their area. This may seem subjective, and it is. Two requirements apply here. First is that the area surveyed is the same every time the data are collected. Second is that the area is large enough to find reported crimes and a good cross section of types of crimes.

When I worked in Los Angeles, I became familiar with many of the police department's processes and policies—some of which were innovative, and some had not changed since Spain had owned the city. Instead of beats, LAPD used Reporting Districts to identify locations and deploy resources. In the downtown and south—central areas where crime was high, the reporting districts were small. On the west side—Brentwood, Bel Air, Pacific Palisades—where crime was lower, the reporting districts—or should I say, "district" was many square miles. There would often be one police car covering an area that took 30 minutes to traverse (on a good day). Ironically, the most vocal citizens, those that paid the most taxes, lived on the west side. Private patrol security was born.

It is also important to establish a time frame for the criminal activity. This may be limited by the source. Las Vegas, for example, only provides 60 days' worth of stats. It would be advisable to go back at least a year to cover all seasons and weather periods as well as tourist and economic cycles.

Police Data and Statistics

If someone sues your hotel, they are going to pull crime data from your local police department going back three or five years, maybe longer. There are two ways of doing this and you need to know the difference to challenge the numbers they might produce. The first method is to accumulate the "Calls for Service." This is what I consider raw data and the police department uses it for deployment, staffing, and mostly internal studies. Calls for Service or CFS is simply the "calls" or activity documented in the dispatch center for the police. Every assignment (shots fired, burglary in progress, traffic accident) is entered into a log. That data can then be filtered for people like you that ask for all the CFS within a mile of your property for a certain time period. Unfortunately, there are several problems with this method of gathering data.

Everything police officers do goes into this log, such as lunch breaks, walk-throughs, follow-up investigations, etc. You might have one incident of a violent crime at your property, but 25 other log entries for back-up, investigations, and so forth.

Another issue I have with these reports is that they list "calls" and not actual crimes. For example, a shots fired call may turn out to be something besides a gun, but still gets counted as shots fired. Many calls to which police respond turn out to be nothing, which cannot be helped, but without some deep digging, you will not know.

The final issue I have with CFS reports is the location. If you have a prominent hotel at a busy intersection, your address will be credited for all sorts of calls that have nothing to do with you, such as a traffic stop in front of your hotel, a traffic accident at the intersection, a fight in the 600 block of Main, or even a homeless person who gets rounded up off your sidewalk and has a warrant will be listed as a warrant arrest at your hotel.

These anomalies in the CFS reports can be a big deal to business owners. I used to be on a city governing body, and we would look at calls at certain bars to determine if they were a nuisance or a drain on resources. For the same reasons I listed above, the bar owners would object to being evaluated in this manner and even forbid their employees form calling the police when they were really needed for fear of ruining their reputation with the City.

My solution to this is to use crime reports instead of calls for service. If the police respond to shots fired and there is a murder or even holes in a wall, they will likely do a criminal report including a case number. This number may or may not get attached to the "call" on the CFS report. If it does, it saves time. If not, I would suggest doing further research. Police reports are public information but that does not mean they are readily available. They get delayed in the system for many reasons. I suggest keeping your own records of nearby criminal activity so you can compare to a plaintiff's research when it comes down to it. Remember that in a lawsuit, the opposing side will pull these reports and use them in whatever way makes you look bad. This is what it is, but your defense folks can also show the difference in CFS and crime reports, and may show, depending what it is, that your security was better than average because your numbers were lower than surrounding properties.

Compiling Local Crime Data

Once the information is gathered, there may be a murder, a couple of robberies, a few auto burglaries, and so forth. This is only the start. For the Risk Assessment, it will be necessary to know time of day, type of business, violent or property crime, etc. It also will be helpful to note the type of security in place at those places for comparison later. (See Table 1.4 for an example of local crime data.)

From our fictional crime data (Table 1.4), we can draw several conclusions with just a cursory look. There has not been a history of hotel homicides, which is why we did not include them in our Risk Assessment earlier in this chapter. Assaults also are not an issue, and judging by the stats, are probably mostly domestic. Robberies, however, are a problem. Of the robberies in this area, 20% were in hotels. Auto thefts were also a sizable percentage of the total, likely because of the nice selection in most hotel parking lots.

Table 1.4 Example of a Crime Data Table

Local Crime Data—Downtown Any City					
Crime	**Daytime**	**Nighttime**	**My Hotel**	**Business**	**Residential**
Homicide	1	2	0	0	3
Sexual assault	3	5	2	1	5
Robbery	10	15	5	15	5
Assault	25	26	4	11	36
Burglary	30	24	6	16	32
Theft	49	54	10	76	17
Auto theft	17	18	5	14	16

Gathering Proprietary Incident Data

Besides knowing what is going on around the property, it is necessary to know what is happening on the property as well. Proprietary data should be the easiest to get. Depending on what types of records are kept, the form they are in, and how long they are held, they can be the most useful. Ideally, the hotel has some reporting system in which data can be mined, sorted, and filtered into what is necessary.

If you are coming into a new property and do not have the historical records that you might expect, then you may need some help. Just as you did previously, consult the local police for their records. This will not have everything (only those incidents reported to the police), but it will provide something with which to work. You might even do this if you do have your own reports because some victims report crimes to the police and not to the hotel. Another dataset to ask for is "Calls for Service" by address. This will give you a great idea of incidents like domestic violence that do not always have an associated police report. The data, when compiled, will look like the police data already compiled (Table 1.4). Rather than create another table, just add the new data to the existing data.

Gathering Market Incident Data

The third type of data needed is market data. This will be the same crime activity gathered previously, but it will be from like properties in the same market. A hotel located by itself may not have neighbors with which to compare, so it has to be assumed that similar hotels in the same region are going to have similar crime activities, threats, and risks. For this research, location of the other property or properties is less important than their type. If the property for which the Risk Assessment is being performed is a multistory, medium-priced resort, then it should not be compared to a budget motel. It is better to find a similar property in another city.

This information can be retrieved online or from the police as explained previously but is best when taken from the source. Security directors who share the same market and have similar crime victims should already be communicating. They certainly should not have any problems sharing anonymous crime data. Unlike colleagues in the sales department, security operations should not compete. Competition when it comes to guest safety does not help anyone and ultimately results in a bad reputation for your region or tourist market. Relationships with peers are discussed in more detail in Chapter 9. Add this third dataset to the existing data. The result should be a table showing what crimes are more likely to occur at our hotel based on neighborhood crime data, our own proprietary reports, and industry averages.

Determining Likelihood

We will use all of the data compiled previously to determine trends and probability. The future cannot be predicted, but history provides a very good view of what is likely to happen. You sports betters or gamers might find that "odds" is a better way to think of likelihood. ("What are the odds of X happening?" or "What is the likelihood of X happening?"—same thing.) Applying this data in a simple list makes some things very clear. In the example

Table 1.5 Determining the Probability of Threats

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious **1 = Least Serious**	**10 = Most Likely** **1 = Least Likely**	**Severity × Probability**
Robbery	8	4	
Domestic violence	2	6	
Property theft	5	4	
Assault on employee	8	3	
Noise complaint	2	8	
Fire	9	1	

in Table 1.5, the Risk Assessment is performed on guest rooms. Not all of the crimes are relevant to guest rooms. Auto theft data, of course, will be used for our assessment of the parking areas, but robbery, assaults, and other thefts may be important to assess risk in guest rooms. These data are objective as they are derived from actual events and require little guesswork or assumptions. The Risk Assessment is almost complete.

In Step 4, probability—or likelihood—is determined. For each event, what is the likelihood (on a scale of 1 to 10) that it will happen? As before, the actual number does not matter as much as the order of events. The most likely should be high on the scale, and the least likely should be at the bottom (near 1). Confusion often arises in this step. Are we to determine the probability of the occurrence without security measures taken, or with mitigation? For example, the likelihood of theft with no lock on the door is higher than if there is a working lock. This will be discussed in more detail later, but for this assessment tool, it is better to determine the likelihood using existing or normal preventive measures. Therefore, when figuring the values in this column, assume that working locks are in place, proper lighting exists, and so on.

In Table 1.5, I assigned a rating of 1 to “Fire” because in my sample hotel there is a no-smoking policy, bed linens meet modern fire-retardant standards, and we have never had a fire in our hotel. “Robbery” and “Property Theft” each earned a 4 because we have had both occur with almost equal regularity and other hotels in our area have had them as well. “Noise Complaint” was rated highest because we are a value-oriented hotel and we get noisy guests all the time. Once again, your values may be different based on your history, type of hotel, and your surroundings.

Determining Risk

The final step of the Risk Assessment is the easiest, and for those visual learners, the most revealing. Multiply the severity value by the probability for each threat to determine risk. In some exercises, you may add these numbers instead of multiplying them. Using the likelihood as our multiplier will give us a broader range of values when we are finished, making it easier to distinguish one risk from another.

In our example in Table 1.6, we had some expected results and maybe a surprise or two. Robbery was high, as expected. Domestic violence and Fire came out low as risks.

Table 1.6 Determining the Risk of Threats

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious **1 = Least Serious**	**10 = Most Likely** **1 = Least Likely**	**Severity × Probability**
Robbery	8	4	32
Domestic violence	2	6	12
Property theft	5	4	20
Assault on employee	8	3	24
Noise complaint	2	8	16
Fire	9	1	9

We probably will not devote as many resources to prevent these in our Security Plan. (Remember, Fire is already addressed in building construction and existing detectors and alarms as per fire code.) "Assault on Employee" was higher than expected. This is a risk that is not always sufficiently addressed in Security Plans, but there are plenty of high-profile examples where housekeepers have been attacked, raped, and even killed by hotel guests. We will address this in our Security Plan later in this chapter.

Insurance companies use this same formula to calculate your insurance premiums. They just use many more variables for severity and probability. Probability factors for car insurance, for example, are driving record, geographical location, age, gender, etc. Severity factors are cost of vehicle, income level, deductible, etc. These factors and others are entered into complicated algorithms to determine what type of risk you are. You can get just as complicated with your property Risk Assessment if you want to take the time. In fact, your business insurance company has likely done something similar to this already.

Foreseeability

Foreseeability is the trump card to the Risk Assessment. Foreseeability means that if an event has occurred on the property before, then it is possible that it will happen again. As mentioned before, history is a good indicator of potential hazards, so if the environment allowed an incident to occur, and the security environment does not change to meet that threat, then it can happen again. This becomes a liability issue. If it does happen again, it will be considered as having been foreseeable by the courts. The event happened because of the inadequate security, nothing changed to prevent it from happening again, it did happen again, and now it is management's fault.

In 1988, a man whose motorhome had been parked in a hotel/casino parking lot in Las Vegas returned to find it being burglarized. The burglar attacked the man and shot him in the head, killing him. The resulting court case progressed to the Nevada Supreme Court on the issue of foreseeability (among other things). The court decided that prior similar acts in the parking lot made this crime foreseeable and that a lawsuit could proceed, holding the hotel responsible for a duty of care to its patron.

Many years later, a man was shot inside a casino in Las Vegas. His estate sued the casino citing the above case that similar bad acts made this incident foreseeable. In this case, the court narrowed the definition of foreseeable to include incidents that were the same (shootings) and that occurred inside (not in the parking lot).

Suppose an incident occurs in the parking garage—like a strong-arm robbery. If basic security measures had been taken—such as proper lighting, security patrol, and emergency call boxes—then there may be a good defense for the hotel in the lawsuit that arises. In most cases, a good security manager will re-assess the area and determine what security measures could have prevented the incident entirely. Perhaps adding cameras, increasing patrols, and gating the entrance points would be considered appropriate. If a similar incident occurs again, there is likely a good defense that the management is doing everything reasonable to prevent such events and protect its guests.

Suppose after the first robbery, the company decides that its security measures are adequate and changes nothing. If a second robbery occurs, the company is going to be in a very difficult position to defend itself because the second incident was foreseeable. The bottom line here is that if you have a violent crime occur in your garage (for example), your security is not adequate. Not every crime can be prevented, but when an event like that occurs you need to re-assess your risk and make sure there is nothing else you could do.

Notice

"Notice" is a term used frequently in liability cases that you need to know. Notice is sometimes inter-changed with foreseeability, but it is a bit different and more specific. Notice means that management or the persons responsible knew or should have known of a hazard or potential hazard. If you are planting a tree next to the main entrance and you leave the big hole in the ground overnight—unmarked, uncovered, and in the dark, then that is a hazard you knew about and could have corrected. Another example that is used commonly is a drink spilled on the floor. Someone "notices" it and cleans it to avoid a slip and fall. Suppose an employee passes by and ignores it an hour before the slip and fall. You had noticed it, so it is on you that the person was injured.

Many companies take this so seriously that they have spill stations around the property and procedures for cleaning it right away. I heard one large retail store do an announcement to its employees, "It is time to do your safety check of your section." If someone slips in a spill that just occurred, it is likely not going to be a liability. The fault is not based on having a drink spilled, but on whether you knew about it and cleaned it.

I will mention this many more times but imagine yourself on a witness stand or in a deposition. Prepare yourself for the questions about security. "Why didn't you have X?" Are you prepared to say that you did everything reasonable you could have done to protect the safety of your guests?

Managing Foreseeability

The word *foreseeability* is not found in many dictionaries. Legal and risk professionals created it and it means that one should have the "ability" to "foresee" events based on previous events that occurred. In other words, if a crime or incident happens, there is foreseeability that it will happen again.

> In 2010, a man who was attacked in his motel room sued a popular U.S. motel chain. The perpetrators had knocked on the victim's door; he allowed them entry and was severely beaten. The suit claimed that the motel chain had a duty to ensure his safety and prevent criminal acts. The plaintiff also alleged that the motel lacked security cameras and patrols, among other things. The motel responded that the attack was "unforeseeable" because motel employees were not aware of the attackers' presence on the property and that there were no known similar incidents at that motel or within the immediate vicinity. The court agreed with the motel, stating that even if the motel had the security measures in place, the crime would not have been prevented because the victim had opened his own door, resulting in the attack.
>
> As we learn in this chapter, even though the motel won this case, they are now on notice. If a similar crime were to occur at that property again, they may be held liable because it is now foreseeable. Strike one.

Some legal professionals refer to foreseeability as the "one-strike rule." The company can defend against that first incident if it was unexpected and reasonable precautions had been taken (strike one). But, the second event is one that should have been expected—foreseen. Therefore, the liability falls more on the property that should have taken steps to prevent the event (strike two—you're out).

The remainder of this book is written with the expectation that security directors want to keep their employees and guests as safe as they can and that reasonable steps will be taken to prevent crime and accidents. Let's be clear on this: Security Risk is not a defense game. We should not wait around for something to happen and then come up with a defense for why it did (some companies do that). In my opinion, we should play offense. Look at every inch of your building and imagine every bad thing that could happen there and then do what you can to fix it. This is a better position for you, but most of all, it is best for our guests and visitors.

Events like 9/11 and October 1 changed the way security directors manage risk. Nobody seriously imagined that planes would be hijacked and used as missiles. And none of us thought that a fellow human could randomly slaughter people from a hotel room. The unfortunate fact is that they did, so now we must change the way we think. It is more than just looking up. It means to me that you must look at your event or your property and imagine what could someone do to cause harm and damage? Is there any possible way for a person to trip on this floor? What impact would a weather event have on this construction site? Out of 1,500 people in your conference center, how many are carrying firearms and what could they do?

Managing Risk

Risk Management is really a function of most security directors. After all, you are the one identifying risks (or threats) and figuring out how to manage or mitigate them. (The Risk manager is generally the claims adjustor at a corporation.) All titles aside, it is important to understand that mitigating risks is rarely anyone else's job but Security's. This is not to say that you negotiate with claimants or evaluate liability. You must be aware of threats, incidents, and trends and take steps to "reduce risk" or mitigate their effects. Make sure your guests are not injured on your property.

Most security directors are reading this and thinking that they have already done their Risk Assessment in their head. This is a great skill, but there are two important reasons for documenting the process. First, collecting written data and compiling it in written form is likely to catch some errors or some omissions that may occur during the thought process. Second, and most importantly, the documentation is vital for litigation. It is difficult to remember and to defend a mental determination, especially if it is years old. If another director or management team takes over, he or she will have no idea how the original assessment came to the conclusions that it did. The written assessment allows the company's legal counsel to show how and why certain security measures were taken if they are challenged. "If it isn't written, it didn't happen."

In November 2005, a man walked into a shopping mall with a rifle, pistol, and guitar case full of ammunition. He shot mall patrons at random, hitting eight of them before being arrested by police. The eighth man sued the mall for inadequate security, claiming the mall could have provided better security measures to prevent the shooting. The mall filed for summary judgment and was at first denied, but upon reconsideration, the court granted the dismissal. The court agreed with the mall that a random shooting in the mall was not foreseeable and the mall had no duty to protect against it. Now that the mall has "notice" of this type of incident, it will likely take some additional security measures (revise its security plan) because it will not be able to use the same defense if a shooting happens again.

The Living Document

The Risk Assessment is always changing. While threats are reduced by the actions in your security plan, risk needs to be re-assessed. Then the security plan will be updated accordingly. Round and round it goes. Using the garage as an example again, you may start out with access control, lighting and cameras as the main components of your security plan. An apartment building springs up behind your property and you have high school kids using your garage as a shortcut. Now you have a new liability (the safety of the kids) and probably some new threats, your assessment changes and your security plan may change to add a uniformed guard during school hours or a wall around the property or whatever works. That all may suffice for a while until you have an assault in the garage and you re-assess. Severity may not change, but probability definitely changes each time an area is fortified. Other factors may change the Risk Assessment. Seasonal factors, demographic changes in the area, special events, economy, regional crime, police patrol, and even the company marketing strategy may change probability and require a new assessment. These specifics will be discussed later throughout the book.

Talking Risk

A couple of terms should be introduced here that are used in the industry and in court to describe risk factors. Let's look at some vocabulary for this chapter.

Duty of Care—In most states, this legal term is the obligation you and your company owe to a guest. The concept is that you have invited a person (everyone inside a soft target is an invitee) so their safety is your responsibility. Of course, this opens up many questions, some of which are explained here as best I can. Others are decided in court, which is why we have litigation. Short answer is, if a guest suffers some bad thing on your property, they may allege that you failed in your "duty of care."

Open and Obvious—This term is used, usually in the property's defense, to describe a hazard that is apparent to a reasonable person. A guest on your property would be expected to avoid something that everyone could see and avoid easily. While everything could be argued, one example might be that big hole I mentioned earlier. Guest falls in the hole and claims they should have been warned. Your company would say, this is "open and obvious."

A woman visiting a major chain hotel in the Midwest went out for a walk during her stay. It had been raining/snowing all day so most ability involving severe pain. The subsequent lawsuit produced several witnesses who agreed the sidewalk was slippery and did not appear to have been "salted." In fact, hotel management did have a procedure for salting the sidewalk but the records of this maintenance were sketchy and appeared to have been doctored.

The award in this case—4.5 million dollars—teaches us three things: (1) make sure that the safety procedure is adequate (salting, in this case did not prevent the fall), (2) if it isn't written, it did not happen. Keep consistent, thorough and accurate records of any maintenance involving safety, and (3) don't even think of doctoring these records to protect your liability.

Assumption of Risk—This is similar to Open and Obvious in that the invitee can obviously see or know the risk and they choose to take the risk anyway. This defense is commonly used in amusement park rides or swimming pools.. If you decide to go in a swimming pool and swim laps and have a heart attack, the hotel will say you took the risk.

Comparative Negligence—When the invitee is partially to blame for the accident. If there is a crack in the sidewalk that could have been avoided and the guest is walking and texting, they might be held to 50% of the "blame."

What Does Risk Have to Do with Security?

Everything. You may have gotten into this business thinking you would be helping people, keeping the peace, and managing crowds. Those are all true, but we can now hire robots to do much of that. We need some analytic professionals like yourself to look at incidents from a "risk" perspective so that we can protect the company from being challenged on those incidents later—and also to prevent hypothetical risk in the future.

As we learned at the beginning of the chapter, this process begins with us looking at what could go wrong and how to prevent it. I call this the "what if…" game and I work it into training of officers and development of supervisors and managers. Besides the formal risk assessment that was discussed earlier, we need to constantly be asking ourselves "what if." This is especially important when our environment changes. New construction, new policies, a special event, concert, visiting dignitary—all need to be scrutinized through a risk (your) lens. For this reason, I try to get involved in every property initiative, attending the planning meetings and participating in design and implementation. It is surprising to me how much non-security folks think they know about risk. Sure, much of it is common sense and is to everyone's benefit to do right, but some aspects of what we do is part of our profession and education.

New construction—the question with a new addition or a remodel is always about cameras. "Throw some cameras up there for security." Many times I have had to have a design significantly modified to put the cameras in the right position and get the proper specs added to them. Your design crew hopefully knows about building and fire codes, but you need to make sure the basics are covered.

A hotel that I worked at before did a remodel on the spa. They called me up to look at camera locations after wire had already been run and drywall finished. They wanted a rubber stamp that I could not provide in good faith. I (politely) made them move things around and add additional cameras. Yes, I removed the cameras from the men's and women's locker rooms, too.

In that same spa, a heat sensor for the fire alarm was placed next to the sauna door. Saunas can get much hotter, reportedly going up to 200 degrees, and heat detectors can be set to as low as 135 degrees. The first day of the new spa, the alarm activated because the sensor was right next to the sauna door and as soon as someone opened it, a rush of heat escaped and set off the alarm. The installers should have caught that but sometimes it takes a different set of eyes.

The more discreet features of new construction are often more of a problem. For example, over the last two decades or so, you may have noticed carpet has been rolled up and replaced with hard floors. Easier to clean, less allergens and dust, and to designers, anyway, more attractive. I found it ironic that when a certain hotel I know installed very expensive, but beautiful marble in the lobby, it became like an ice rink in inclement weather. Rain or snow being tracked into the main doors made a muddy and puddly mess which required a full-time housekeeper with a mop to keep clean. Management's solution? Put down those high traffic outdoor carpets from the kitchen to catch the wipe water from people's shoes and distribute several yellow "wet floor" signs. Italian marble and plastic safety signs—how beautiful.

If someone had said at the outset, I think marble may be kind of slippery and we may be paying for some broken hips, they might have reconsidered. The compromise could have been a rougher tile or an additive to the varnish that makes it less slippery when wet. I see the same irony in nice public restrooms. The tile is a glossy marble or similar in an area where people walk around with wet hands, shaking them on the floor looking for towels. One solution again is to put the signs down. An unfortunate unsightly solution.

The security team is uniquely poised to notice things like this—quite frankly because they have to deal with the injured guest. I used to love the feedback I would get from sending security out to assess certain areas of the property with a fine-tooth comb. Yes, they came back with some outlandish "what ifs" but they also brought some legitimate hip-saving suggestions for improvement.

Special Events are another area where security needs to be involved from the very beginning. Our event organizers do not always think about crowd movement, potential emergencies, and other what ifs. I would often tell our folks to just let me know their intentions and I would do my best to make it work. If you go in and say NO to everything, they will simply stop inviting you. An Incident Action Plan, which is discussed in more detail later, will allow you to assess your risk in advance and come up with ways to mitigate it before the event occurs.

I could cite hundreds of scenarios from cases I have worked, where a bar, restaurant, hotel or other venue continue to have the same problem over and over again, and continue to ignore it or do nothing about it. This is risk-gambling in my mind, because you already know the bad thing is going to happen, but you are risking your business, your employees, and your guests that it does not happen tonight. Or if it does, you will not be held responsible for it. It just takes one guest who is an innocent bystander at one of your Friday night fights, or slips and falls in one of your dozen nightly spilled drinks, or is assaulted by the coupon distributors that you know are in your hotel, to sue you for several days' worth of revenue.

It is not a recommendation or suggestion, but an obligation you have to your guests to assess risk on a daily basis as follows.

Reacting to Risk

When an incident occurs, reverse engineer it and see how it could have or would have been prevented. Cleaning up spills in a timely fashion, adding extra patrols to the hotel hallways, making sure the room doors close and latch by themselves, adding lights to dark areas, and on and on. In most cases, this is a simple process and where your training, and this book, will pay off. Many of these physical security best practices are contained throughout these pages.

Remember we introduced Foreseeability just a few pages ago? This is where the wax meets the floor—so to speak. If you do not re-assess a hazard after an injury or incident, you are doomed to repeat it. You may be able to consider that first incident a random fluke that has never happened before, but you cannot say that about the second—or twelfth.

Frankly, I found this to be an enjoyable part of my job and I was pretty good at it. I trained my folks to be good at it also. After certain incidents or claims, we would meet up, either formally or informally, and figure out what went wrong. Was it entirely the guest's fault? Even if it was, is there something we could have done to at least help prevent it? We not only did this with accidents, but also fights and other man-made incidents.

Pre-emptive Risk Assessments

The pre-emptive risk assessment is the one that prevents the accident because we took action before someone was hurt. The Risk Assessment explained at the beginning of this chapter of course does the same thing, but there are smaller assessments you can do on a continual basis just by observing the actions on your property. Perhaps you observe the same drink server walk across that marble floor 20 times per shift sloshing to and fro. This may be a training issue or a procedure to be revised, or maybe a reason to move the bar.

The old days when we opened up a business and started counting the money are long gone. There are some responsibilities that management has—and security as an arm of management—to its guests. Ignoring the car burglaries in the parking lot, watching employees cut their fingers on the deli slicer, taking reports of guests falling in the shower, are all unacceptable. It is up to us to prevent these incidents from occurring.

This goes beyond mere injuries and gets more serious if the threats are more severe. If you, as the security director are reading reports of incidents that occur over and over and no mitigation is being done to prevent the incident, you are not only negligent, but liable and, arguably, inept. Or it may just be one incident that could have reasonably been prevented. Or there may not have been an incident or injury at all, but several near misses. You still have a duty to take some reasonable action to make sure it does not happen. A simple example is a tear in the carpet that you walk atop every day. No one has tripped, and it has been there for months. The risk assessment is: Is it likely someone could trip? Yes. Are they likely to be severely injured? Probably.

Even though this was not specifically covered in your initial property assessment, it needs to be analyzed in real time—not with a volume of paper, but a simple decision that says, let's fix this.

Managing Threats

We will not be using the Threat Assessment (TA) in determining Risk. The TA is used on a specific subject, such as a stalker to determine if he is a danger and what should be done with him. Having said that, we still may use a TA for a political convention, certain concerts, and things like that.

However, when doing a general risk assessment, whether it is for a building, event, or company, the threats can be so overwhelming that we end up back to an "all-hazards" approach to managing them. For example: suppose you are in charge of the protective detail for the president. A week before the next public event, a threat is received that says a bomb will be hidden in a trash can along the motorcade route. A threat assessment is made, the suspect is an ex-military munitions expert and lives close by. Obviously the detail you supervise will take all sorts of precautions to prevent this bombing. Does that mean they will not be prepared for a sniper? Or a different bomb scenario? Or a close quarter shooting? Of course, they will prepare for all these things whether they have any specific threats or not.

Of all the mass casualty incidents in recent memory, which ones were accompanied by a threat? Pearl Harbor? Beirut Marine Barracks? Pulse Nightclub? World Trade Center? Even the JFK and Reagan shootings. In hindsight, each of those incidents should have been prepared for the method of death that faced them. Easy for me to say, right? I did not even mention all of the school shootings, commercial shootings, and other mass murders that have occurred. What did they all have in common? There was no threat—at least not one that made it to the proper authorities. If nothing else, October 1 needs to teach us that we will not get a warning when someone wants to come and do bad things. They will just do it. There is probably some psychological or sociological explanation for that, but I am a results-oriented practitioner and I say we better start preparing for everything we can imagine and then prepare for things we cannot.

We are good at preparation after the fact. Look at what we changed after 9/11. Ship placement was changed after Pearl Harbor, presidents do not ride in convertibles anymore, and so on. Las Vegas Sheriffs, Hotels, and many event-venues changed a whole bunch of stuff after that shooting.

It sounds expensive and time-consuming, but it is not, necessarily. It is going to take some awareness, a culture change, and that "all-hazards" approach I mentioned. Remember the little list of major incidents I made a couple of paragraphs ago? If you were going to plan each of those events or protect those locations now, it would be minor tweaks. For example, armored limo for JFK and better security of high places, moving the ships out of the harbor, and tighter policies for the hotel. It is all do-able without time and expense. Awareness is the key. We are doing all those things now, so we could have done them before, but we just did not know.

Rick Rescorla was a colonel in the US army before retiring to teaching and then Corporate Security at Dean Witter in the World Trade Center. After the 1988 bombing of an American commercial jet over Scotland, he convinced himself that the WTC was a future target for a terrorist bombing. He called in a colleague and they assessed the building security, deciding that a truck bomb in the basement could topple the entire tower. Their warnings to the authorities in New York and his superiors were ignored and in 1993 Muslim terrorists did just that. A truck bomb detonated in the basement, causing damage and a few deaths but was otherwise a failure for the bombers. Rescorla was convinced that the WTC was too attractive a target and even predicted a plane crash into the buildings in an attempt to bring them down. He even went undercover in many NY mosques to gather intelligence about the former and future bombings. Since his bosses still would not cancel their lease in WTC he insisted on evacuation drills for all employees. He did this every quarter until 2001 when the planes struck the towers. Rick personally directed over 2,600 of his employees down the stairs to safety against Port Authority orders to stay at their desks. He was last seen going back up into the burning building to get stragglers before it collapsed.

Another point about threat assessments for large events. Doing a TA on one person who has a few knucklehead stalkers is hard enough. Doing that for an event with 20,000 people is impossible. If you are looking for someone with a motive, you would have to look at the friends, family, spouses, and enemies of all 20,000 people. Just doing the country singer has proven not good enough, because we have seen how killers attack their victims within a large crowd or event and take along some collateral damage.

Many of the Questions that Came from Media and Others after October 1

Why did he do it? Why did it happen here? Who is to blame? What could we have done different?

Allow me to give you the answers if you do not know. He did it because he is crazy. Maniacs hear voices and every once in a while they follow them. It happened in Las Vegas because that is the city he knew, it is one of the most prized targets in terrorism, and it happened at that venue because it was right next to a hotel he knew well. Fault? Really? It is the fault of one guy who is dead forever. There are many things we could have done different—if we knew then…But we did not. Now it is time to lose the denial, folks. We did this after 9/11—blaming all sorts of people and we do it every time.

Yes, I do have a solution and some recommendations. First of all, forget about motive. It does not matter. It is a curiosity but it does not help us prevent anything. Second, investigate the threats but do not put all your eggs in one basket. Every one of these types of incidents was a surprise. Nobody said I am going to be there at 10 p.m. and start wailing on you with a gun. Even terrorists do not claim responsibility until after the fact. Third and most important, plan for every type of incident you can imagine and then plan for the ones you cannot imagine. Plan for everyone dying, plan for hospitals to be closed, plan for a tsunami to follow an earthquake (Fukushima), plan for police to abandon their police cars and run home (Katrina). Then plan for a global pandemic on top of all of it—our new normal.

Reasonable Steps

The reality is you cannot prevent every possible threat or bad thing that will happen. What is required of you is to think of every possibility and do what is reasonable to protect your guests. For example, we now know it is possible for someone to use your hotel room as a perch to shoot thousands of rounds at thousands of people. If you were in Las Vegas or a similar city with outdoor festivals, it is more likely than in a rural area and a 100-room hotel. However, you do need to take some reasonable steps, such as room inspections.

Those reasonable steps become best practices, unless they are not reasonable. Going back to our October 1 example, the week after that shooting, one major hotel chain announced that it would eliminate the Do not Disturb sign. They decided that daily room inspections would be a reasonable step to prevent someone from setting up a gunner's nest like that guy did. Ironically, and perhaps to my point, during the Corona Virus pandemic, many hotel chains adopted the policy of no room cleaning during your stay (only upon check-out). Even though that is opposite of the previous best practice, the virus was considered a more likely threat, so it will be around until the pendulum swings back.

A best practice can last for decades, such as peepholes. Or they may be brand new like the covers they put on those peepholes after an infamous case of stalking. It is your job, to stay abreast of these practices and continually update your security based on current trends.

After the October 1 shooting, I was interviewed by a prominent news organization about the future of security in hotels. One of the questions was: Will you deploy glass-break detectors on all of your hotel rooms? In my opinion that is not a reasonable solution to that situation—for many reasons. The room inspection solution is more effective, timely, and easier to manage.

Do not be tempted to latch on to the latest and greatest software or technology that is designed to prevent or detect certain threats. Ask yourself the what-ifs… If I have a shooter up in my hotel, and he breaks the window to start shooting, is glass break detector going to prevent anything? Ask yourself what if I had inspected that guy's room in the past three days, or what if my employees did not help guests up a non-guest elevator, and so on.

This is just an example of how a best practice is enacted. There will be plenty more along the way. I urge you to investigate mine, discuss them with people important to you, and offer some of your own to your peers.

SECURITY PLAN

> The plan is to make sure my daughter is safe. And the only way to do that, so it seems…is to eliminate the thing that will make her unsafe.
>
> *Taken 3* Movie

Security Plans exist for several reasons. Some places require them as a matter of law. Large Corporations may require them. An on-the-ball CEO or GM might require one.

Bars in New York must have a security plan to get a license to sell alcoholic beverages. Having seen some of these, they are one page and copied from one property to another. Not even a formality, security plans of this type are rarely followed, created by someone who knows nothing of security, and are filed away with the liquor license by the owner.

Large corporations that have an appreciation for the protection of their assets and/or understand the duty owed to their guests will have a fairly comprehensive security plan—and follow it. Capital expenditures will be held against the plan, and other expenses and policies you attempt to pass through better align with the plan. I actually agree with this concept but it's a frustrating one when the plan you have to follow is not yours or it is so outdated that it becomes a hindrance.

Finally, it may depend on who your boss is. I have had one that pulled that plan out of his second desk drawer every time I was in his office to ask for something. You bet I kept it up to date (once I caught on) and it really worked out well. Or you may have a more passive leader that says just make sure it is done right and they have no interest in your plan. (They probably do have an interest, but they empower their subordinates to supervise themselves. And that's OK with me also.)

Do not assume that because you run a small venue or facility, that you do not need a security plan. A security plan may be a 100-page document, or a one-page set of notes. It applies to a barber shop and a 4,000-room hotel equally. Security measures are basically the same, it is the scale and maybe the potential losses that change. But does it matter if a deadly drunk driver got intoxicated at the fancy bar in a large hotel or in the small bar around the corner? We will address all the above going forward. Sometimes I will explain the large and the small of it, and sometimes it will be up to you to apply these concepts to your particular operation.

Crime Prevention

In the previous chapter we looked at risk and how to determine what it is. Now, I take you back to your police academy, your community college, or even your woodshop days to discuss prevention. There are many illustrations that describe prevention methods. I want to expose you to two concepts to which I will refer throughout this book.

The Crime Triangle

Law Enforcement uses this illustration to explain how to prevent crime. The concept is that a crime is a result of three factors: Environment or location, the suspect, and the victim. If you take away any one of those factors, the crime cannot happen. For example, suppose you have a rash of car burglaries in your parking lot. Applying the crime triangle, you take away one of its legs. You can set up a stakeout and catch the person committing the thefts (take away the suspect). You can educate or re-direct the car owner so that they do not leave valuables, park in valet, lock their car, etc. (take away the victim). Finally, you can improve the location. Add lights, cameras, security patrol, gates, etc. (fix the location). This is more than academic. It just works. It is up to you, however, to figure out how to eliminate one side of the triangle. We will dive into some examples of the triangle in the upcoming chapters.

The Physical Protection System

The Physical Protection System or PPS has been around for many years and is now an industry standard. It is used in court, used to implement a security plan, and this book embraces it.

The PPS consists of three components that work together to become a comprehensive set of security measures that protect the property and its assets. The three components are Human (personnel), Policies and Procedures, and Technology (or resources). I generalize technology because a rock can be part of a PPS. If you look at the PPS for an automobile that keeps you safe, you have the driver, traffic cops, the engineers that designed the car, repair persons, etc. That is the human element. Policies and procedures that pertain to a car's safety are traffic laws, driving instruction, minimum requirements for seatbelts, brakes, lights, etc. Finally, the technology is addressed by anti-lock brakes, anti-collision sensors, cameras, and even the roads themselves.

Whether it was planned or not, most of your security systems include all three of these elements. Leaving one or more components lacking is like selling your system short and could be considered negligent. Using only one or two of the components will likely result in failure and it leaves one to question whether you did all that you could to protect the area and its personnel. This book and others about Security can help you complete your plan to include more of these elements.

The parking lot with the burglaries that I used as an example earlier is again in the spotlight. Suppose you had really bright lights protecting the lot and that's it. The burglaries are still occurring and then someone gets attacked. You are going to be asked why you left so many opportunities to protect that lot un-addressed. Why didn't you have cameras? Human patrol? Access control? Parking restrictions? Signs? Etc. These failures to secure may be considered negligence.

I hope to give you some ideas, recommendations, and suggestions that will help you round out your program and keep everyone safe. By the way, do not get caught up in the expense. There is no comparison between life safety and spending some money on security. It is not as bad as you think anyway, but way worse than you think if you find yourself in court because you could not shell out a few bucks.

What Is a Plan?

In an ideal security world, we would take our Risk Assessment and come up with a perfect plan to mitigate every risk. In reality, the plan you create and implement will be influenced by your style, education, and experience and that of your manager and maybe your lawyer. That is why I do not presume to tell you how to run your department or your property. Instead, I offer some proven methods, best practices, and even some unusual ideas that I have seen or tried myself. It will be up to you to apply the ones you think will work for you and your property. That is what a Security Plan is and what this book is all about.

Remember that with every new technology or security measure you consider, you will have to explain to someone why you need it and someone else why you did not. For example, suppose a new technology was developed to identify active shooters as they walked in your door. For several reasons, you decided to pass. Then an active shooter comes in and kills people. Now you are back on the witness stand explaining why you did not install the technology. It does not mean you were wrong, but you need to be able to justify your decision. This is what keeps Security Directors up at night: Did I do enough?

The security plan is a document that explains what security measures will be taken to mitigate risks (prevent crime and accidents) on and around the property. This process is a bit subjective for hotels and entertainment venues because the standards and best practices are often passed along informally and individually. This book attempts to gather them and organize them for more common use and knowledge. In an airport or nuclear facility, there are government regulations that standardize access control and other physical security aspects. Hotels, amusement parks, nightclubs, and similar facilities are not so regulated. Fire and building codes, Occupational Safety and Health Administration (OSHA) guidelines, and other applicable regulations address much of what we need, but cameras, lighting, security staffing, and other security measures are not included. The hospitality industry has not yet standardized physical security either. However, there are some best practices and corporate policies applied by larger hotel chains, and there are practices that arise from litigation as well as some government agencies who have come forward with acceptable standards. These will be used throughout this reference and should be used whenever possible in the security plan.

Remember, as with risk assessment, the main purpose of documenting the security plan is to justify the security posture of the property when it is challenged. Since there are few standards and one-size-fits-all practices, your security is sure to be compared to that of a property with "better" security. So, for the purposes of this plan, the best practice will be recommended every time. Your goal is to provide the best defense (security plan) that you can within reason.

Accident/Incident Prevention

When an unfortunate event happens on hotel property, the victim of the act often names the hotel in a lawsuit. The victim sues the hotel—not because the hotel caused the act, but because the hotel did not take adequate measures to prevent the crime or incident from occurring. It is for this reason that the risk assessment and the security plan are so important. The plaintiff's lawyer will try to find where the security was weak or below standards. Since some standards are vague or general, the only way to prove substandard security is by comparing to other properties, examining best practices, or considering what would have been reasonable. The risk assessment will show where the other properties were examined and the security plan will show that industry standards or best practices were utilized, or left out for good reason, and that every reasonable step possible was taken to protect the guest.

Part of our job in security—in addition to keeping guests safe—is to help defend the company against claims. Incidents and accidents are going to happen on your property, and it does not matter so much whose fault it is as whether it was preventable. Sometimes it is not preventable, and we gather as much documentation as we can to assist our Risk manager with settling the claim, but also to help us identify things we need to correct or improve so the same accident is avoidable in the future.

Prevention is usually not the sole responsibility of Security, but since we are on the front lines and see most incidents, we can make recommendations for change. Other departments or individuals may have to be involved. The Risk manager, perhaps the general manager, Facilities, Finance and safety, should all be reviewing your reports, and making their own recommendations. At one place I worked, we had a "risk group" that met weekly to discuss the prior week's incidents and resolve safety hazards, claims, and any other issues that come up with security reports. I recommend this process, but like any other regular meeting, bad habits will develop if not kept structured. If the risk manager is settling everything before the meeting, then the other attendees will deem it a waste of time, which it may be, in that case.

Smaller businesses, such as a bar, may have one person (owner/manager) that wears all the hats described above. Because the corner bar is smaller than a major hotel, they should have less incidents. The owner/manager can always sit down with a trusted employee and brainstorm ideas on how to deal with a claim. Regardless of the size of the facility or number of incidents, it would be a colossal waste of time to document and investigate without taking any corrective action.

Decisions

Many factors go into the decisions to make physical or systemic changes to your property as a result of an incident. It is security's responsibility to address criminal threats—and sometimes third-party accidents—while the person in charge of property maintenance or Risk may make changes to flooring, handrails, and other areas. Making a physical change to the property begins to complicate things. I think an interesting example is the "Great Hotel Bathmat Dilemma." Yes, I am exaggerating, but you would not know it to see some of the conversations I have witnessed between Housekeeping, Risk, Hotel, Facilities and Safety on bathmats. For those of you that are not up to speed on the bathmats, it goes like this. People who stay in hotels tend to slip in the shower/tub on occasion. These falls get blamed on the soap, the surface of the tub, presence of handrails, and the rubber bathmat. I have seen bathtubs re-surfaced, shampoo swapped out for less-slippery brands, caution signs, and many arguments about it. The bathmat gets pulled, moved, eliminated, re-stocked, and the circular bathmat dilemma is born. If you spontaneously make a change like adding bathmats to the hotel rooms, it could affect prior claims or litigation, housekeeping's methods of cleaning tubs (and mats), how they are presented to the guest, how they are cleaned, etc.

That was just a fun example that I could not resist. A more serious example would be that you decided to re-direct security manpower to a certain area where teenagers are coming in after school and vandalizing vending machines. You had to reduce patrols of the swimming pool to accomplish this and as soon as you do, someone drowns in your pool. Although the vandalism likelihood was high, it rates low on severity—especially compared to life safety. A drowning is the highest level of severity, but the likelihood was lower. On paper they almost even out, but always include in your decision that life safety, no matter how likely, is first. Keep this in mind as we create the Security Plan.

Building the Plan

When I started in the casino industry in the last century, they used what I called "the shotgun" method of security planning. That included putting up 400 cameras, hiring 150 security officers, and copying the procedures used at the other casinos. They got sued all the time and lost—or settled—because nobody assessed risk, and nobody considered the hazards inherent to the property. I call this the shotgun method because throwing a bunch of security out there not only lacks precision and efficacy, but also is weak on objectives.

Objectives are going to be the keystone of most of the processes contained herein. We tend to buy technology and decide how to use it later or hire a bunch of people and schedule around that number. When a new casino is built, they over hire by about 50%. As they figure out how busy it is going to be and how many employees they need to run the facility, they start laying them off. Though there are some advantages to this (like having extra just in case, being able to comfortably weed out the bad employees, and de-stressing management who do not have to worry about scheduling), it is lazy, expensive, and unfair to those that get laid off after 30 days. Of course, new projects, like casinos, tend to have a bunch of start-up capital that they must use, so it might as well go toward extra labor.

Casinos are not my point. My illustration is about having an objective. If someone had taken the time to calculate how many dishwashers, how many food servers, how many security, and so on, they would hire the number they need—or pretty close to it.

The Security Plan is the objective (or list of objectives) for the security department. It is the "what" that we are going to do: "Provide a visible security presence in the garage"; and a little of the "how" we are going to get there: "Roving patrols, call buttons, access control, lighting, etc." The method described here for the plan starts with the objective and works backward to figure out how to get there. I use this process whether I am writing a policy, planning a trip, or organizing a meeting. Decide your objective first, then plan to get there.

Did you ever attend a meeting headed by someone who has no objective? They call a meeting because there is a problem—or a situation—and he wants to talk. The meeting starts out well, with an explanation of the problem and then it turns in to arguing, griping, telling jokes, talking sports, and generally getting off track. Where were we? Objectives. Even if the meeting is a brainstorming one, you need an objective or you will drift. More on this later.

We cannot create a Security Plan until a Risk Assessment has been completed. The plan includes security staffing amounts, cameras, lighting, access control, CPTED (crime prevention through environmental design), and many other physical aspects. It may also include policies and procedures. Many organizations create and follow unbelievably detailed and lengthy plans that explain and outline all these pieces of their security posture. Other, maybe smaller, properties do not make a written plan. Most security directors are either operating under a plan written by a predecessor or do not have a written plan at all. They rely on their mental notes and personal philosophy to create policies and organize their protective measures.

Like the Risk Assessment, the Security Plan is not valuable unless it is written. Those who do not have a written plan simply have not had to justify their security to their boss for the purposes of obtaining funds for staffing and hardware. They also have not been deposed on their justification for why they had a certain level of staffing, certain video or alarm systems, or policies that did not address certain aspects of security. The formal Security Plan is not that difficult to write and may save time and money later.

Beware of the opposite situation: You will be held to the plan in court. If you document that you need X number of personnel and you are running with a lesser amount, you just shot yourself in the foot. So the wording we will use when writing the plan will NOT include words like "always" or "shall." We will use words like "may" or phrases like "when possible" or "when safe to do so." If your objective is to have someone patrol your garage every two hours, do not put in the plan that you need 10 officers to do that. You may replace walking rovers with bikes or Segways or even robots.

Most of the remainder of this book is a security plan. So you know which information to include, here is an outline you can use to create your plan.

Outlining the Plan

If you have ever written a business plan, you are at an advantage because it is remarkably similar. Your company probably updates its business plan every year and it can be very complex to include marketing, forecasting, employee benefits, capital improvements, etc.

Security is similar but focused, of course, on security. If you still have no idea what I am talking about, here is a method of producing the plan. Take a look at your Risk Assessment. (If you were too lazy to write that, jot down the threats to your business and your guests.) The threats become your objectives: "keep unauthorized persons out of the basement," "only allow hotel guests on the hotel floors," "make sure guests have safe passage to parking lot." Write them in a column, and next to each one list the ways you will address those threats. For example, humans, cameras, alarms, locks, etc. The second list will look like, "install cameras," "provide security patrol," "install access control," and "increase lighting."

Once you have this spreadsheet of sorts, expand it some more to include details such as how many cameras, what kind, location, how are they monitored, recorded, etc. Other details may include: How many officers to provide patrol? What is the frequency? Riding bikes? A car? How many access points? Who has access? Access control with gates and locks, electronic system, etc.

If you do all of this for your entire property, you will have quite a document so far. This "list" includes the Personnel and Technology components of our Physical Protection System. Now all we need is that other "P," Policies.

Part of the Security Plan will be a Policy Manual. We are going to write a manual later, but the outlines for each are similar. Is this circular logic? No, the manual is part of the plan but the plan is not part of the manual. Makes perfect sense.

Department Mission
Organization
Policies and Procedures
Overall Property
Specific Areas
Each of these components of the Security Plan is explained in more detail.
Department Mission

> If work has no intention, it's not work at all. It's an empty motion.
>
> *Razor's Edge* Movie

Most of us consider the Mission Statement a bit corny and a throwback to the days of team-building, organizational changes, and employee empowerment. Whether you have one, want one, or neither, I would like you to have a few of my opinions on the mission statement and see how best you could apply it internally at your place.

Most companies have a mission to keep them on track when making business decisions and to commit to their employees and customers that they are set on their objectives. "…market leader in widget-producing in the Northeast area…" Each department must have a mission that supports the main mission. "The manufacturing department will increase output to meet the mission of the company…"

- The mission statement is the overall strategy of Security for the property or organization.
- The security mission statement must support the company's mission statement.
- Security is how a company meets its mission, not the mission itself. If the company's mission is to be the market leader in guest satisfaction, and your mission is to be the best trained force, then those statements do not align. They could, but they do not. Security's job is to support the company's objectives and the objective is to increase guest satisfaction, then you need an objective that is relevant. Security's mission is to provide a safe atmosphere and tend to guest's concerns so that they can enjoy their stay.
- At the very least, I want you to have a mission in your head. What is your general objective? Maybe it is not so obvious. Some major hotel chains focus on reputation and the corporate standards. Take a look at Disney. They are very focused on "magic," "Be our guest," and appearance. Security does not conjure up images of these warm, family objectives, so they put security officers in themed uniforms and train them in guest service, taking pictures and greeting children. The security that is necessary, but not aligned with the mission is kept out of sight.
- Rarely do you see a company that says, "We will strive to be the safest hotel with the fewest accidents and least crime of any other hotel in the industry." But the hotel that says, "We will provide a world class experience with attention to detail and anticipation of our guests needs" cannot get there without security that has similar objectives.
- Where is your company trying to go: luxury, high volume, great value, brand, etc.? Then you need to know what the company expects from security. I worked at one hotel whose mission for security was "prevention"—reduce crime, high visibility, keep bad things from happening. The mission of this hotel was something about high value and family fun. That attracts a different kind of guest and the security department had to be prepared for the "budget-minded families." The security department focused on managing large crowds and a higher potential for crime and bad behavior, so they had more visible uniforms, police-style training, and a culture to match.
- Another hotel I was fortunate to manage had guest service and luxury in their mission. They had softer uniforms, hardly any training, and a service attitude and culture. So why not have all of these things as your mission? You can try, but there will be a priority on one and the other will suffer. And I guarantee, the budget-minded hotel will not want to waste time on amenities and white glove service. The Luxury hotel will not tolerate a SWAT team on their payroll.
- Reading the mission statement of the Ritz-Carlton, you would have to assume that the mission of their Security Department is consistent with the hotel's mission of "finest service" and "unexpressed wishes." It is likely that security's mission is something along the lines of discretion, comfort, and service that supports the objectives of the hotel. As for Southwest Airlines, their Security Department probably focuses on the keywords in the corporate statement like warmth, service, and friendliness.
- Consider looking at other departments to see what they have.
- You also may talk to those who wrote the corporate mission statement and get ideas from them.

- Finally, as I mention throughout this book, ask your own employees to help develop your mission.
- Your mission statement is not just something to hang on the wall; it will be used to make important decisions on the type of security used throughout the property. Refer to it each time you make a decision or create a policy. This will help you remain consistent.

ORGANIZATION

Organization of the Security Department includes the chain of command—or hierarchy—from executive down to front line. The purpose of this section is to make clear who reports to whom and who has which responsibilities. Names are not important—just positions. Why is this important in the plan? One reason is that those who read this plan (lawyers, your boss, and your successors) need to know how decisions are made and at what level. Do frontline employees operate on their own, with minimal supervision, relying on management from other departments to make important decisions, or is the organization large enough where there is a shift manager to whom officers report? This may be a vital component of the plan when, in court, your company is trying to defend a poorly made decision.

There may be other uses for this chart as well. Your Controller may use the pyramid to determine how many employees at what salary range are employed and included in Cost-of-Living Adjustments. The Human Resources (HR) department may use this when they re-structure or merge with other companies for forecasting and aligning operations. Benefits may use it if there is a progressive benefits plan or bonusing for management. And like everything else, this document is likely to be subpoenaed when you get sued. It may be used against you or it may be a defense for you to show proper staffing and span of control (explained later).

Starting at the top, who has the highest, or ultimate, responsibility for security matters? This depends on the corporate structure, the size of the organization, and the corporate philosophy. Many companies have an executive security position reporting to the CEO or the property manager. Some companies have the security leader (director, manager, etc.) reporting to Legal, Human Resources, or Facilities. There are good reasons for each reporting structure, but that reasoning is probably out of your control. So, for the purpose of the Security Plan, we are simply documenting it, whatever it is.

This organization chart is going to look somewhat like a pyramid and since we started at the top, we will work our way down. Next is the second line of management. Large organizations use an operations manager in this senior middle position. It also may be divided between operations and investigations or administration. Instead of having two managers in this position, the Ops manager can take the Personnel/Operations side and the director can take the Administrative or Investigative side. The director is still the highest authority, but it saves a position. (It is advisable not to have two persons in charge of the entire operation.)

I am aware that some readers do not have a security force large enough for this many layers. As I mentioned earlier, the book looks at the extreme, in many cases and lets you scale it back. Even if there was only one security officer in your hotel, he/she needs a chain of command with a reporting structure, even if they are not security employees.

The above level can be skipped entirely if the organization is small-to-medium in size. The third (or second) tier is middle management. This position could be called supervisors or shift managers, depending on the number of frontline staff. The ideal proportion of supervisor to officer is 1:5. So, if there are ten officers on a shift or team, there should be two supervisors. This is not to say that if the property has decided to use a "shift manager" format, that two managers are needed per shift. It means that each five persons need a supervisor, so this can be accomplished through different levels of supervision.

The next level might include supervisors (if managers are used above) or senior (lead) officers. If a property has 15 officers on a shift, there could be a manager and two or three supervisors, or a supervisor and three senior officers.

Keep in mind that a small property may not have many levels of supervision in Security. If there is one officer on duty at night, he or she may report to a hotel manager or similar position. However, your ideal ratio depends on the size of your property, the skill level of your employees, and other factors. This needs to be drawn out in the organizational chart as well. Almost every property, regardless of the size of the force, downsizes at night—or upsizes on weekends. This must be included in the "pyramid." If there is one manager/supervisor on dayshift, does it go down to zero on grave? Hopefully not. There should be some position that has responsibility for every position below it.

If you are operating a 25-table restaurant or a bed and breakfast with five rooms, you are likely balking at my numbers and my organization. As I mentioned before, scale it back to fit your needs. For a small operation, you simply need someone in charge.

V.A. Graicunas developed the term *Span of Control* in 1933 when he researched the effectiveness of varying management ratios. He determined that there were several factors, such as the physical location of the employees (whether they work together or separately), personalities, types of work performed, and the capabilities of the employees. That ratio was found to be acceptable at 4 employees to 1 supervisor all the way to 22:1 depending on those factors. Police departments operate at about 4:1 and fire departments operate at about 3:1.

In the 1980s, a new factor was found to influence the effectiveness of this ratio: technology. Computers and other automation systems took away some of the duties of supervisors and managers, and many corporations "flattened" their chain of command. Middle management positions were eliminated as duties were given up to technology. We still look today to eliminate middle management as one way to save money. Some really progressive companies have flattened their chain of command almost entirely. This socialized form of management encourages "group thinking" and everyone is fairly equal with few supervisors, if any.

The final level—the base of the pyramid—is the officer. This is the front line and the most important because they do the most work.

The organizational pyramid likely includes other units of responsibility besides Operations. Investigations, Training, Administration, and Safety are common units to include in your chain of command and organizational chart. Others included in some hotels are Lifeguards, Lost and Found, Shuttle Drivers, Parking Attendants, etc. Whatever legs of your pyramid you might have, each must have an "upline" and a "downline" of who reports to whom from the director on down. We will explore some other ways of adding levels to the pyramid—or moving them—later.

One important note: Be careful with the numbers that your chart represents. If you present a chart that represents your max staffing level to a lawyer that is suing you for inadequate security, you are going to have to explain why you did not have the staff that your chart says you need. I think you can avoid this situation if you either leave the numbers in each position at a minimum or have different charts for different business levels.

JOB DESCRIPTION

Each of the positions described previously and each position held in your department requires a job description. The purpose of a job description is to outline the job functions of that position. This description may be needed in litigation, for progressive discipline, coaching, training, promotions, new positions, and light-duty determinations.

A job description is relatively simple to create, and your Human Resources Department may have already done this for you. Following is an outline of a generic job description.

Position title
Department
Pay range
Reports to
Subordinate positions
Minimum qualifications
Physical requirements
Hours or schedule (if applicable)
Job functions
Revised date

HR probably already has a template so fear not. But you may find that they really do not know what a security officer does, besides walk around. For example, an officer may be expected to kneel for long periods (doing CPR or cardiopulmonary resuscitation) or climbing some stairs (fire alarm). These tasks will come into play for injuries and subsequent medical releases. When all the job descriptions are complete, all the duties under your authority should be documented. If anything is missing, that will explain where you lack accountability.

I took over a security department that had several people on "light duty" which meant they had chronic or permanent disabilities that were protected by the Americans with Disabilities Act (ADA). While it was nice to be able to employ some great people with some unfortunate setbacks, I was not able to effectively provide for the guests to whom I owed a duty of care. When I spoke to HR, they explained that ADA requires them to make "reasonable accommodations" to those with disabilities. We would have to show a need for having stricter requirements. Unfortunately, our job description was vague and could have been the same one for a front desk clerk.

We re-wrote the job description with some clear requirements, such as climbing stairs, kneeling, lifting a certain weight, etc. We even included loud noises, enclosed spaces and heights. We did not fire any of the existing employees, but we did make sure that when they left, they were replaced with an able-bodied security officer.

Your HR department likely has language they prefer that complies with the American Disabilities Act and labor boards and agencies. This is why they probably have them written for you. If you want to update or add something, make sure you run it by them.

I used to tell my frontline staff that they worked much harder than I and that I did little more than go to meetings and work on budgets and things. Many of them would quip back, "Then why do you make so much more money than we do?" My answer: Because the higher you go on the corporate food chain, the less duties you have, but the more responsibility is bestowed. I got to take credit when they did something good, but I likely would get my butt chewed if they did something bad. I used to ask my peers who were "covering a shift" why they were wasting the company's money putting a director in the position of a supervisor or officer. One cannot manage if they are on the front line.

POLICIES AND PROCEDURES

The policy manual will be explained in the next chapter, but your security plan needs a few words on Policies and Procedures. There will need to be some basic policies that dictate how security will function in each area so that it can be applied later in the plan. This may involve other stakeholders. The Risk Manager (legal counsel), the General Manager, and affected department heads may have a say in how security operates and performs certain functions.

Before any policies or procedures can be written, several questions need to be addressed.

What is the Security Posture going to be? Posture is a word I use to define how security is going to act and be perceived. Is it going to be aggressive, crime-fighting, friendly, luxury, passive, visible, invisible? Though the word "posture" is used figuratively here, I can give some literal examples to show the differences in security posture.

1. You have likely seen a "bouncer" in a club or at an event that had a tight black shirt that displayed his muscles and fit body. The posture at a place like that is obviously, "ready," "aggressive," "ass-kicking," "low tolerance."
2. Perhaps you have been in a museum or a high-rise office building where the security officers wore black suits with ties. This uniform indicates "class," "dignity," and "we will not be having any trouble here."

3. Posture is not only about uniforms. Some venues do not have any visible security at all. They are likely working undercover or behind the scenes. This is common in department stores where asset protection is the focus, or amusement parks where everyone is on stage.

So the question you need to ask yourself—or your boss—is what security message am I trying to convey? It is not about personal preference—or it should not be. It depends on all those factors in the risk assessment. It depends on the demographic of your guests. It depends on the location and environment. And it depends on the brand and reputation of your organization.

When a property I know wanted to upgrade their uniforms, Security was told that they had no say in the matter. The type and color of uniforms was going to be decided by the owner's wife! She was "coordinating" uniforms with the carpet and drapes. In my opinion this is the wrong way to go but may be a fact of life where you are.

Once you have decided on a security posture, the rest of the questions should fall into place.

What is the Use of Force Policy? Many departments try to simplify force with a couple of words like "hands off" or "shoplifters will be prosecuted," but they fail to back it up with a comprehensive policy, training, resources, and hiring. Whichever end of the spectrum you decide to adopt, you must back it up. The secondary question here is guns? No guns? Tasers? Pepper Spray? Batons? This is way more complicated than you can imagine and we will look at all sides later.

Will you use Contract Security (or contract police) or proprietary employees? (Or none at all). Many companies make the mistake of hiring a guard company and assuming they are no longer accountable for what goes on or how issues are addressed. We will go into this in detail later, but your plan needs to know now.

Many of us are results-oriented directors. We want to take care of business. We would rather be out there greeting our guests and working alongside our employees instead of writing a bunch of stuff no one will read. Rules and regulations do not bother us but writing them does. Our gut tells us that many of the things we need to document should be common sense and should not need to be written. The truth is, the written security plan and its associated policies come with many negatives: Discipline, Worker's Comp limitations, and litigation defense. Fortunately, there are some good reasons to have a plan. So, take some time and get this part done right. It may save your job, protect your company, and it will definitely keep your guests and employees safer.

Overall Property

Your Plan will include an overview of the property. This is likely a sketch or drawing or even a CAD. Remember that your property—and security—does not stop at the perimeter walls. Include all outside areas—and maybe even public streets and sidewalks if they are relevant.

The drawing should include, generally, the security layers installed and proposed. Cameras, lighting, guard shacks, gates, alarm systems, etc. Putting this in a visual form will assist you in making sure that nothing is missed and makes it easier to explain to others. It also gives laypersons a better understanding of what is going on.

It is not necessary or advisable to provide too much detail or to give away proprietary information. Some physical measures change from time to time, and you do not want to have set yourself a standard on your plan drawing that you cannot keep. You may end up using this drawing for an incident action plan, or an emergency planning requirement. If by chance, an outside agency shares it, you do not want any private information there.

Specific Areas

These are drawings of specific areas on your property such as the Lobby, a sample hotel floor, parking lot, etc. These are drawings you are less likely to give out so I would put more detail into these. Locations of cameras, IP switches, alarm panels, are all good notations to make on these drawings. Again, these are helpful in planning projects like camera locations, wire runs, VIP evac routes, and other security functions.

Are there special elevator controls? Door locks, software used, panic hardware, bulletproof or bomb-resistant glass—anything that is an enhancement for security. If you have tamper-proof cigarette butt receptacles, even they are a security enhancement.

I am a visual learner (like many of us) and I like to see a project laid out before me so I can imagine how it will look and to see if anything is missing. If you are not a visual learner, someone in your audience may be, so I recommend as much visual detail as possible.

INCIDENT ACTION PLAN

The Incident Action Plan is like a security plan for just one event or period. Most of the components of the plan are temporary and may be new or unusual for the property. This is a concept I stole from FEMA (Federal Emergency Management Agency) and our local emergency management folks. “Stole” is not the right word because FEMA is very generous in the forms and classes around those forms. In fact, if you have not taken advantage of any of the government’s free training, please go to fema.gov and explore. None of it is for sale, so if you stray into a dot.com that wants to sell you something, go back to FEMA.

Though I got this concept from the professionals, I modified the form and most of the information for the private sector. Check with your local first responders and see if they will share a sample with you. Better yet, see if they will count you in on a planning meeting for an event. You will learn a great deal. Meanwhile you are stuck with me.

The Incident Action Plan is a planning document for a planned event. This has nothing to do with emergency response or recovery. It is created before the event, not after. I have found, as in most planning that the process is more useful than the document itself. Like many exercises we do in this book, you create your plan by talking it out with your colleagues (stakeholders). This is practical and real. If you are not doing this already, please try it.

The process starts with a meeting well in advance of the event. (By the way, the event can be anything from a wedding reception to a street festival.) For our purposes, we will talk about events where security plays a major role. You may have meetings like this already—like a pre-con or special event meeting. The folks planning the event may already have something written, but they will likely not include the things you want in there.

Of course, start the process with the facts—demographics on location, crowd size, times, dates, invitees, etc. Then include more detail about the event. Is it outside? Streets blocked? Parking lot? Inside? Convention area? Type of music? Tickets? Etc.

Now we have some security questions, don't we? This meeting is where you need to find out. Are you hiring contract security? Police? Emergency Medical Technicians (EMTs)? Are there VIPs or celebrities that require special attention? How do they get in and out? Will there be searches?

Those line items that cost money will likely have to be approved by the General manager or GM. That may put you in a difficult situation because generally, the special event folks do not budget for security. If they did, it would likely be lower than you want. You can stay clear of this argument between the GM and event planners. Once the financial compromises have been worked out, you need to memorialize these meetings with a document—The Incident Action Plan. Cruise the Internet to find a sample that you like because it does not really matter what format it is in, but that you can read it. It should also look professional because just like a report or your policy manual, it may end up in court.

The October 1 massacre in Las Vegas will be used as an example throughout this book. Imagine holding an outdoor event with 22,000 attendees, dozens of police officers, hundreds of security officers, medical technicians, and the rest. You would need to plan how to deal with fire, active shooter, weather collapse, crowd control, medical emergencies, triage, first responders, access control, talent security, and many other facets. You cannot just do this in your head, and even if you could, you have to share it with those hundreds of staffers to be on the same plate. Admittedly, things do not always go perfectly and there are unforeseen threats as we learned that fateful day.

SUMMARY

Note that with the security plan, like most of my illustrations in this book, I start with an objective and work backward through challenges and details. This ensures that we stay on track, are in line with the company's goals, and do not waste time and money on things that do not help us reach our objective. Though I speak most of the time about large hotels and corporations, these tools apply to the small business owner as well. Any business that exists for the purpose of providing entertainment, comfort, or leisure—yes, bars, that is you also—should take these recommendations and use them on a smaller scale.

The Risk Assessment identifies where you need to go, and the Security Plan tells you how you will get there. They may be read by your Risk manager, CEO, Corporate Counsel, outside counsel, plaintiff's counsel, judges, security experts, consultants, and some members of your team. If written poorly, they do more harm than good, but if they are thoughtful, accurate and comprehensive, these documents may protect you and assist you. Stay tuned as we explore the planning process throughout this book.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

2

Policies and Procedures

Though we introduced policies and procedures in the last chapter, now we will work on writing them.

HIERARCHY OF RULES

When I teach classes on How to Write Policies and Procedures, I still get some blank stares: What is the difference? P and Ps are the same things to many people, and other terms are completely misunderstood. So let's come to some agreement on our vocabulary because they are different and it does matter. When we define words like "crimes," "practices," and "rules," it is tempting to use words like "severity" or "penalty." I will kind of use severity as a sort order, but really they are best defined by how many they affect. Stand by while I explain that.

Laws, codes, ordinances, regulations, standards, best practices—there are so many "rules" we have to follow. But really, we do not have to follow most of them and many do not apply to us so it is not as complicated as you might fear. Let's break it down and get past some of the confusion.

REGULATIONS, STANDARDS, AND OTHER LEGAL MUMBO JUMBO

We have criminal laws and civil law here in the US. Obviously, one is directed at persons and results in prison or fine and the other can apply to entities or persons. Since the government cannot arrest a business, it will generally go after the leadership. Businesses can commit crimes but are generally punished financially or systematically. Laws can be enacted by a city, township, county, tribe, state, or other governing body. Within the hierarchy of laws, the Constitution, and its nephew the US code are the highest laws in the land and therefore affect everyone. The states have adopted more detailed, and often more restrictive, laws that are prosecuted at the state or county level. After that, it starts to get

DOI: 10.4324/9781003037644-2

more complex, but generally, each level of government (county, city, township) can write its own laws.

Crimes—Crimes are acts or omissions of laws. Without getting too deep, a crime is legislated and codified in a document like a penal code. Crimes include homicide, theft, disturbing the peace, etc. There are federal, state, local, and other crimes, but most are misdemeanors prosecuted at that level of government. A controversial example of this is gun possession. The Federal law is the second amendment of the constitution which is arguably vague on possession ("right to bear arms"). Many states have restricted that law to make guns illegal in certain buildings, and other such prohibitions. All of this is not so black and white, which is why we have lawyers and judges, but my point is that crimes apply to the entire citizenry depending on the location.

Codes—These are also rules (or crimes in some instances) that are applied specifically by type. A code is generally a compendium of many rules that apply to the same topic, such as a fire code or health code.

Ordinances are laws adopted by a municipality that only apply to a local area like a city-wide parking rule.

Regulations are industry-specific laws enforced by an authority, such as a liquor authority. Codes, ordinances, and regulations are still laws which may be criminal, but they are enforced locally and specifically. They apply only to those they affect (bars, in the case of liquor, for example).

If criminal law is one side of our illustration, Torts are on the civil side. Torts are violations of common law—or case law—and include Negligence, Emotional Distress, Financial Losses, and injury. To prove the cases for the above torts, plaintiffs will argue violation of the law or failure to follow or adopt other "rules" that are not criminal.

Industry Standards—Standards are not laws, but generally rules imposed by an industry on itself. They only apply to the industry (businesses) and the penalty may be no greater than exclusion from the industry. An example of a standard is the ratings on movies. If you allow your 12-year-old to attend an R-rated movie, there is no jail time or ticket or police officer waiting at the door. Movie ratings are set by the industry and imposed on moviemakers and theaters. (Hold on to this thought as it will become important throughout this book.)

Best Practices—Practices are not rules or regulations at all, but techniques or methods that have proved to achieve the desired result. A best practice may come about in our industry from a trial where it was proved that a certain practice was the "best" way to do a certain thing. A good example of a best practice is the manual that we are going to create in this chapter. Nobody says you have to have one, you will not be arrested if you do not have one, and there is no fine to pay if you don't have a manual. It has simply been proved over thousands of court cases that a documented manual of policies is a good defense in court as well as a valuable training tool. I put this category here because these practices likely dictate—or should dictate—how your company and department operate. Ironically enough, the policies contained in your policy manual are likely all best practices and a few standards.

The other big difference among practices, standards and laws, is that industry standards and best practices may or may not be written. Some of them have been taken on by associations like ASIS (American Society for Industrial Security) and the AHA (American Hotel Association), which turn them into standards. Putting the word "standard" on the document header does not quite make it one. There is generally input, feedback, and consensus from a group of experts and practitioners. Anything that made it that far surely represents us well and should be followed.

Best Practices do not go through the same scrutiny (unless they want to grow up to be a standard). They travel by word-of-mouth, and via publications and books like this one. You can be assured that the practices in this book are "best" and I will tell you when they are not. Otherwise, you learn of best practices from networking, industry journals, and seminars. So how does this affect me?

Let's look at an incident and see if we can place different levels of responsibility on it.

Suppose a guest is knocked down on the stairs leading up to your hotel. Her purse is stolen in the process and she gets a broken hip. This is a crime—a felony—committed by the perpetrator. The hotel has no criminal liability. Now this woman has some medical bills, and she was told this was a safe area, so she files a lawsuit claiming some sort of noncompliance with a law, a code, an industry standard, or a best practice (or multiples and combinations of the same).

From the information we have, the hotel did not violate any laws. If they had, the lawsuit would be over before it began. There are building codes and fire codes that may apply, and if one of those was intentionally violated, that could also be a quick end to the suit in favor of the injured. Since those possibilities are unlikely, the plaintiff will probably go after your Physical Protection System. That is when security experts are hired by both sides to opine on whether the hotel could have applied industry standards or best practices to prevent the crime, or whether they did everything within reason to protect its guests.

Note that our "ladder" of rules started at the Constitution and ended with Best Practices. This was meant to show you the difference in requirements and recommendations. It is also to illustrate that many of your decisions as to how your operation runs are subjective. You would not knowingly operate a hotel in violation of the law and risk jail time. I would hope you would not violate any fire or building codes that put guests at risk and cost you fines. Yet each day, for reasons I will soon explain, some of us choose to ignore industry standards because we think we can. Best practices, too, get ignored because there is no "penalty" until we must defend these decisions civilly.

It is much easier to complete this risk exercise before something happens rather than in court. The risk assessment is how we do this, formally. Leaving that front stairwell to your hotel unprotected is like deciding to wear your seat belt. You are taking the gamble that nothing bad will happen. I called this risk-gambling in the last chapter and the term fits because they are both about money. If a crime can be prevented by spending money on lighting or investing in security officers, the reason we normally do not do it is because we do not want to spend it.

There are other reasons we "neglect" security. One is ignorance. We just do not pay attention to the potential problem—or are too lazy to address it. The third reason, in my opinion, is vanity. We think it will make our hotel look bad to have too much security or it will upset our guests to see that we are worried about crime. So, rather than judge, this book will show you that there are plenty of things to do that cost very little, are invisible to guests, and that are widely accepted and proven to work.

In 2002, Casinos in Laughlin Nevada hosted a biker event that was widely attended, including by opposing gangs. What had historically been a relatively peaceful event turned deadly when one gang went into the same casino as their rival and started a fight. One gangster was stabbed to death and two more were shot and killed. In addition to the numerous lawsuits against the casino, security at the subsequent events was substantially tightened. One remedy was a "No Colors" policy because vests and bandanas and things were believed to contribute to the violence.

In 2011, a casino in Sparks, Nevada hosted a portion of a regional biker event for the first time. This shooting involved one of the same gangs and a third one. It also started at a casino bar and resulted in one dead gangster. It seemed that the casino had learned nothing from the prior incident and did not adopt the *best practices* that were initiated after 2002. (No Colors, bolstered police and security presence, and segregation of rivals.) The following year, a Nevada Hotels association officially deemed the No Colors policy to be their industry standard. As explained in this chapter, the standard does not compel any hotel to follow, but the association can distance itself from the rogue entity. Worse, if that hotel were to have a shooting or other gang-related violence, they would have a hard time defending why everyone else was following the standard and they were not.

Elements

Now we switch gears back to laws. Every law has at least one element. In order to arrest, charge, and prosecute someone for a crime, the elements must be proved. If one is missing, it is either a lesser crime or no crime at all. The state I hail from had a crime called "defrauding an innkeeper." This law likely derived from a very strong resort influence because it specifically protects the property from theft and other nuisances. If someone eats in a restaurant and leaves without paying, that could be a "defraud," but the elements have to be proved.

The elements of defrauding an innkeeper are: (1) taking or using merchandise, food or accommodations; (2) from a hotel or other business; (3) with intent to defraud (not pay). So, if someone enters the restaurant without any money, consumes the meal, and refuses to pay, then all the elements are there, and the charge is good. If he never gets his meal—no crime. If he leaves, thinking his friends are paying—no crime. If he mistakenly believes the meal was part of his room rental—no crime. If all three elements do not exist, it becomes a civil matter, and you can negotiate a "settlement." Sir, we need to figure out how you will pay for the food you just ate.

In some states, grand theft auto (GTA) has a secondary crime commonly referred to as "joyriding" because many kids steal a car just to drive around and leave it somewhere. This did not meet one of the elements of GTA, which is "Intent to permanently deprive," so they made a law that excludes that element. This was also done with homicide as there are degrees of intent, from accidental, to negligent, to heat of the moment, to malice aforethought. If you watch Law and Order, you know there are differences in manslaughter and homicide.

Your coffee shop manager might chase a guy through your hotel, finally catching him in the lobby, only to find that he was going to get his wallet he left in his room. This is not only embarrassing, but could constitute battery, false imprisonment, defamation, and a host of other issues requiring a defense.

The intent of this section was to keep you out of trouble with the police and the law. It is common for an employee, or even your boss, to define some behavior or act as criminal. While it may seem wrong to them, its criminality depends on the location. Public intoxication or drunk and disorderly is only against the law in some states (i.e., Nevada and Colorado). In other states, it may be prohibited, but individual cities allow it (New Orleans). This is just one example of why we need to know which laws apply to us and what the elements are.

There are a few laws that you will find common for our industry or at your property specifically. Please see how your local law enforcement agency handles them, so you do not do something that will be used against you later.

Even laws are of several types. Federal laws, including the Constitution, apply to everyone in the US. We are not familiar with many of them because local laws generally replace them, which I will explain shortly. Federal laws include things like sexual harassment, equal rights and discrimination, and many of the labor laws we follow. Other criminal laws we may be concerned with on the federal level are copyright, patents, and Native American reservation laws.

Most states and tribes adopt their own laws. This is done so that the state can prosecute their own criminals in their own courts. Generally, felonies are prosecuted by the state, and include those laws that apply state-wide, including homicide, sexual assault, theft, robbery, and so on. These differ only slightly from state to state but you should be aware of the elements for each of these crimes in your state or jurisdiction.

Your municipality, whether it is a county, parish, township, or city, may further create laws—sometimes called ordinances—that apply in that jurisdiction.

Firearms laws, as I have seen them, are some of the most varied among states and cities. Some states are very loose with firearm laws, allowing unrestricted sales and carry, while others are very strict, prohibiting many sales and carrying altogether. Still, in some states, there is inconsistency as well. One city may have tough restrictions, while a rural county in the same state will have less restrictive laws.

The reason I explain this is that one may wonder if someone can carry a gun into their hotel, or keep it in the car, or bring it to the hotel room. Knowing the local laws is only half of the answer, as it comes down to hotel policy.

Generally, as the jurisdiction gets smaller, the laws they can enact can be more restrictive, but not less. For example, a township cannot say we will allow murder under certain circumstances. A state may, however, make a federal law more restrictive. They have degrees of murder that outline the severity of the murder, changing the elements. The following crimes are those we encounter in a hotel or entertainment venue.

Homicide
Kidnap
Robbery
Arson
Sexual assault
Battery
Domestic battery
Assault, aggravated, with deadly weapon
Burglary
Theft
Vehicle theft
Embezzlement
Trespass
Defrauding innkeeper
Fraudulent use of credit card
Forgery (checks, currency, etc.)
Fake ID
Identity theft
Alcohol (dram shop) crimes
Retail theft
Firearms carry
Other weapons

As you can see, we encounter almost every type of crime, and the list is incomplete. We will discuss some of these laws individually elsewhere in this book.

Codes

The waters will start to muddy now. A code is a compilation of rules that are adopted as laws. The best example I can give you is the International Fire Code. This code is created by a private entity (not the government) and derives from years of updates, multiple expert contributors, and its relation to other codes. Without government adaptation, it is merely a guideline or standard. Most fire departments accept the code in its entirety or perhaps make some modifications and then they go to their legislative body (a city council, county commission, etc.) and ask for it to be accepted as law. When it is, of course everyone has to follow it.

One example that pertains to us is the recent update that requires crowd managers in areas of assembly. This code requirement will be explained later, but for this section, it means that in 2018, the IFC (folks that write the code) added it in, the fire department liked it, and your municipality made it a law. The Health Code is similar in its evolution and there are building codes and other codes that may apply to you. Just like you did with laws, I recommend communicating with that enforcement authority to see how it affects you (health inspector, fire inspector, etc.)

Standards

Standards, as I mentioned above, are guidelines that have been officially agreed upon, reviewed and adopted by some association or organization that is considered the expert for that field. Security has ASIS that establishes standards. There are some hotel associations that have a few standards, but most have stopped short of creating standards. One does not have to follow a standard unless it is dependent on their membership in a certain organization. The hospitality industry has no standards that apply to every hotel or tourist venue. That is because most hotels do not align with a particular association. What does this mean for us? Good news and bad news. Bad news is that there is no official resource for you to determine how you are supposed to do something. The good news is that there is no official resource for you to determine how you are supposed to do something.

Let's take nightclubs for example. Everyone always asks what is the proper ratio of security personnel to guests in a nightclub? 1 to 100? More? Less? If you have a nightclub, you know it varies. It is dependent on clientele, music format, size of club, number of exits, history and reputation, and so many other things. This is why we do a risk assessment and develop a security plan. Otherwise, I would write a very short book with some data and numbers for you to staff.

Guidelines

Guidelines are the same as standards, except that they may not be widely accepted by the end user. Not that there is something wrong, just that they have not been researched and accepted by a wide body of participants.

Best Practices

This is where the hospitality industry lives: Best Practices. Just like it sounds, a best practice is a method or procedure that has been accepted as preferred. It is just like a standard, except it has no shiny gold seal attached. But seriously, we deal with best practices every day. Sometimes best practices are proven in court. Here are some examples.

Electronic key locks are a best practice. Nobody made us put them in, but we all realized it was the way to go to keep guests safe and secure in their rooms.

New York Police and other police departments have published best practices related to security in nightclubs. Even though these are from the police, there is nothing that says you must follow them, but because most venues accept the practices as best, if you do not go along, you may find yourself in trouble.

Hourly patrols of the hotel. Whether you do this or not, I can tell you that many court cases come down to how often you patrol your hotel (or other parts of your building). Hourly or every two hours is commonly accepted as the norm for hotel patrol. Of course there are other factors and more often would be better but you should always be prepared to explain why.

Handcuffing. I really like this one. Did you know there is no law or even a standard that says you must put someone in handcuffs when they are arrested? However, it is so widely accepted as the best safest and most effective way of restraining someone, that we all do it.

Deviating from a best practice is dangerous. If you do so, and something goes wrong, you will have to defend your reasons for doing it your way. For example, if you are operating a nightclub without a dress code or weapons policy, you are legal, but if someone gets shot, who is going to be under the microscope?

This too is a compilation of best practices. While I have some opinions and there is subjectivity to everything, I will always try to note if my recommendations are best practices. Assume that they are, and I will tell you if they are not.

Company Policies

I include this in our hierarchy of rules because policies are more easily enforced, you have complete control over them, and you do not have to arrest or call the police. Policies should be developed to cover any bad thing that you want to prevent in your property. For example, if a piece of jewelry came up missing in Lost and Found, is it easier to charge an employee with theft? Or terminate them for failing to follow Lost and Found procedures. A theft accusation must include those elements which are intent, knowing he or she committed the theft, plus you must have a victim. But if they just did not log it into the system, you have a policy violation.

Our goal is to protect assets, not enforce laws, so write policies that do just that. Weapons is another one. Most of the laws regarding firearms are related to public property, not private. So if you wanted to prohibit guns in your lobby, make a policy and do not rely on a law that may or may not exist to do that for you. Same with marijuana. There is no law that forces you to allow someone to smoke marijuana in their hotel room. Surprised? People think they are entitled with decriminalization, but private property still trumps those laws (usually).

The next three rungs of the hierarchy ladder are the company manual, the department manual, and the training and emergency manuals. These and the incident action plan are discussed next.

TYPES OF MANUALS

Policy vs. Procedure

The words "Policy" and "Procedure" have different meanings. The words do get grouped together, especially in a manual so that no one knows the difference. If you are not clear on the exact meanings of these two words, I hope to change your life right now.

Policies are "what" and Procedures are "how." Policies describe what the company wants to accomplish—or their objective. Procedures outline how the company—or department—is expected to follow that policy. Example: Company policy says, "Guest Rooms will be checked every three days." The procedures would be, "Housekeeping will knock and enter a room on the third day even if there is a DND. Manager or security will be called if door is locked. Housekeeping and Security will make every effort to reach the guest by phone prior to opening the door," and so on.

If you are still not with me, try this. The policy is the place we want to be. Procedures are how we will get there. Imagine your CEO setting a policy of "Firearms will not be allowed in the building." This is an objective—a gun-free hotel. It is general and simple. The security department might be tasked with enforcing this policy, so you create procedures to identify persons with guns, how to approach them, what to do with them, etc. What do we want and how are we going to get there? A policy and corresponding procedures. There.

Note in the examples above that the policies may be in the company policy manual and the procedures may be located in the respective department Procedures manuals. As I mentioned before, policies and procedures are usually combined into one book. The policy may be listed at the top of a page and the corresponding procedures listed below it. The other option is to have a "Standard Operating Procedures" manual (SOPs). This may be an appropriate way to document your procedures if the policies are listed elsewhere.

Security may have four or more types of manuals. (Do not freak out: they may overlap and repeat in some cases.) The company manual, or corporate manual, contains the policies for the entire organization. The security manual is the comprehensive set of Policies and Procedures (objectives) for the Security Department. The training manual is the guide used to train employees within the Security Department. The emergency manual applies to the entire organization but is specific to emergency preparedness and business continuity.

Company Manual

The company manual is a set of rules for the entire company. This may be a corporate manual that applies to all properties in a chain, or it may be a property manual that applies to all departments at that property. There also may be both: a corporate and a company manual. Of course, this manual sets the rules for every department to follow, and generally only those rules that apply to all departments. This document is usually created and maintained by Human Resources, company counsel, or a specific regulatory department.

In most organizations, the company manual is used as the guideline or framework for the department manual. Where the company policy might dictate general policies, the department manual will expand those policies into specific procedures. For example, most hotel companies have a general appearance and grooming policy. This policy may require business attire, neatly groomed hair, and a presentable appearance. Then each department will expand on that to address uniform standards, hair length, beards, moustaches, piercings, nails, etc.

The company manual, which was already written by someone else, might make a good outline for the security manual. Keep this in mind when the security manual outline is discussed later in this chapter.

Another company manual is the regulatory manual. In the casino industry, there are minimum internal controls that set guidelines for all aspects of gaming. The cruise line industry follows several similar documents relating to maritime and Homeland Security regulations. Then there are rules and contracts for unions, trade groups, conventions, health and fire codes, and many other rules and policies that may have an effect on hotel policies. These documents, like the company manual, will provide a framework for many of the procedures for the Security Department.

Creating these company or regulatory manuals will not be discussed in this book because the Security Director is not likely to have this responsibility. However, as mentioned previously, these manuals provide the guidance to produce the Security Manual.

Security Manual

The security manual is the book to which we will devote most of this chapter. It is simply a book of certain policies and procedures for the entire Security Department. You may prefer to call it an SOP manual. You may also decide to combine it with the training manual. I think this gets complicated, so I do not recommend it.

I cannot emphasize the importance of a procedures manual strongly enough. If you do it right, keep it current, and actually use it for daily operations, it will help you in many ways. If you go with the dusty book on the shelf, it may be used against you—with great success for the plaintiff.

> There was a lawsuit against a hotel whose security officers used excessive force against a man for whom they had no criminal charges. They broke his leg, denied doing it, then tried to justify it, then ignored it. The hotel, whose name you would know, and whose manual you would expect to be detailed and an industry standard, was an embarrassment. There were more pages devoted to administrative tasks than there was to guest safety. The policy was actually a reasonable one, but it was clear that the security officers had not seen it and had not been trained on anything in it. The director, when deposed, had to defend a manual that he had not written and then explain why his staff did not know its contents.

The need for a current and complete security manual is based on consistency. As explained in Chapter 1, the manual is an asset for defending the hotel in court. This value will only come when the manual is followed consistently. To ensure this consistency and strength of the manual, it is produced in three steps. First, the policy or procedure is decided and then sanctioned by management and counsel. Then it is organized and documented in the manual. Finally, the employees need to be educated on its contents and apply the rules in their relevant daily tasks.

I wrote my first manual for the company where I worked in the early 1990s. I was so proud and confident that it was comprehensive and would protect our guests, our officers, and the company. I learned a few lessons in the following years and taught myself to build an effective, useful manual.

One thing we did wrong was we had more than one manager working on several manuals simultaneously. Another manager was building the emergency manual while the training guy was creating his training manual. As you might guess we ended up with three good documents that were well-written but were not consistent. Put them all together and try to make sense of them and you would be lost.

Another big stumble I had was that I did not have anyone outside my department to review and comment on the policy manual. It ended up being a thick book, and though I assigned my managers to read it, they did not. If I had an expert read it, or someone that had written one, it would have contained many things that I omitted.

The manual was put to the test at my first deposition and a couple after that. I had things in the manual that my staff did not know or were unsure of. We still had many "unwritten rules" that turned out to be important.

The final lesson I learned was to avoid language in the manual like "always," "must," shall, etc. Using absolutes takes away discretion, exigent circumstances, and special events or special guests. If some violent incident occurs at the front door of your property and your manual says, "There shall always be an officer posted at the front entrance," you will have a problem convincing anyone that your manual contains your real policies or just those that make you look good. "So if this policy was not followed, how many others in the manual are optional."

Training Manual

The training manual is a necessary tool often overlooked in Security Departments. Its purpose is not to dictate policy, but to detail the procedures of each task that follows a policy. The training manual follows the outline of the procedures manual, but details the steps of each procedure. For example, a security manual might explain the policy of reporting employee accidents. The training manual would give the security officer step-by-step instructions for completing the paperwork, gathering evidence, and conducting the investigation.

Building Your Manual

The best way to write any book, including a security manual, is to start with an outline. (Remember those term papers in high school? Me neither.) It is really not so difficult, and you can use the example in this book to get you started. We will go through it systematically in order. You may add, delete, or modify certain parts of the example to meet the specific needs of your department. As I have used my own manuals and taught classes, I have changed my outline many times. So do not hesitate to vary from my content as you may have better ideas. There is an outline at the end of this section to use as an example or template.

Foreword

This first section of the manual, before section one, is not about policies or procedures, but is more of a warm-up to what the department and manual are all about. Naturally, it will start with an introduction. This is a brief summary of what the manual is about, how it is to be used and updated, and who the intended audience is. Remember we talked earlier about security posture. This is a good place to explain your security posture. Your objectives, the company culture, and things like that. Like an opening statement in a trial, use this medium to sell and explain your objectives. You want readers to understand that your intentions are honorable and good. Safety is your prime directive.

Next might be the mission statement of the department. The mission statement was discussed in Chapter 1. Here it is placed in its official form as the guide to the department's policies and procedures.

Finally, I suggest a welcome to new employees. This should be in the form of a personal letter from you to them.

> This security team came together 10 years ago for the purpose of protecting the assets of the hotel. We hope you enjoy working here as much as the rest of us and if you should ever need anything, please do not hesitate to ask me or any member of the management team.

Or something like that. This is not required but I believe it sets a personal tone that is the foundation for morale. Be grateful and complimentary of your staff whenever you can.

Department Policies—Section 1

The first section of the policy manual is appropriately devoted to the most important policies of the department. These policies are critical enough that each employee signs them as part of his or her on-boarding process. These policies, probably already written, include your Guest Service Policy (hopefully this is your most important), your Confidentiality Policy, and others such as Sexual Harassment Policy. Please don't tell me that those are handled by Human resources. That is exactly how we insensitive security guys get in trouble. Guest Service is everything to this department. Confidentiality is vital to a successful operation. If you still think sexual harassment is an HR problem, then how are you going to expect your folks to give a damn? Duplicate these policies as the main pillars of your department. Live by them and pound them into heads daily. Maybe you have some others: Discrimination? Conflict of Interest? Whatever is important to your company, put it in there. If you have only one employee, these documents and this section are still important.

Organization—Section 2

The next section outlines the organizational aspects of the department. You may want to include an overview of how the department is set up as it relates to reporting, accountability, and responsibility. The chain of command will be an organizational chart: department head at the top, and the succession down to the frontline officer. Be sure to include other branches, such as an administrative assistant, investigators, trainers, etc. Finally, each position or job will need a description. Even if you have two employees, you should at least list those employees with their contact information. We already did an org chart and job descriptions in the security plan and HR likely has them anyway. So we have already gotten two sections into the manual and we have not had to write anything yet.

Employee Policies—Section 3

This section includes every rule, procedure, and guideline relating to the conduct of your employees. This is where each employee learns what is expected of him or her. In the example, we start with new hire procedures—how new hires are selected, the interview and vetting process, and the training required in your department. This section will not include every training syllabus, but will include the requirements for each skill level. List how many hours are spent on each training topic. Time spent learning how to reset the fire alarm is not going to impress anyone. Hopefully the majority of training time is spent on force, de-escalation, safety checks, and so forth.

Based on my travels, appearance is not as important to others as it is to me. If it is not a big deal for you, or if you have no staff to show off, then leave this out. If you do, put what is acceptable and what is not. These policies become subjective and difficult to enforce when they are not in writing and easily referenced by supervision and officers.

Include all of those rules that have been passed on verbally and in writing by email, meeting, and memo, and are flying around all over the place. These are technical policies like accepting gratuities, break times, and dealing with guests. When I get behind on this section, I go back through emails and memos and look for those “effective immediately” rules. (How many times has your policy on tattoos or piercings changed in the past 20 years?)

Discipline is probably already a company policy, but very necessary to include in this document. A good policy manual is the first place a supervisor should look to find out how to discipline an employee. Outline the “ladder” of progressive discipline, what constitutes a unique ladder and policies that have no wiggle-room like attendance.

Termination is coincidentally after discipline in our outline. This section may include the final step of discipline, but also the procedural aspects of how to give notice, where to obtain the final check, and clearing out desks, files, and computer logins.

Scheduling is the final section in this chapter. Included are rules on attendance, call-offs, which holidays are paid, how payroll corrections are handled, breaks, and light duty. Any rules associated with an employee’s schedule or paycheck should be included here. Light Duty has become more complicated than I ever imagined. Consult your Benefits or HR folks on what is right to publish on this topic. Most of these topics apply equally to small businesses, in fact they may be more important because in a small group, lines are often blurred on rules.

Posts/Patrol Areas—Section 4

As we will learn in Chapter 5, posts are any place you have an officer assigned, whether it is a fixed post or a patrol area. This section will list each post with a description and the post orders for each. This may be the longest part of your manual, as it will include posts that are not covered all of the time. Even the bar with two bouncers needs job descriptions and post orders. Some caution needs to be given to staying on post. This is explained in Chapter 10.

Systems/Procedures—Section 5

These are the "operations manuals" for each system used in your department: reporting systems, CCTV, and everything else technical. You also will describe and explain how to perform various procedures in detail, such as lost and found.

Crimes and House Policies—Section 6

Arrests

Types of crimes (misdemeanor versus felony)—The textbook definition of the different elements of the two (or three) crime types and the differences in when to arrest.

Searches—The Fourth Amendment, case law, state law, and company policies on when to search, how to search, and the associated liability and safety issues. Where are arrestees held and what is acceptable conduct from them and around them. How are issues dealt with like "one phone call," bathroom breaks, etc.

Use of force—The Use of Force Policy, when force is justified, how it is applied, and the consequences for doing it incorrectly. So many companies leave this out of the manual—in fact many of those do not address force at all. Even if your policy is "hands off." You need a UOF policy. This is explained in Chapter 3.

This section includes a list of the commonly used laws associated with hotel security, such as trespassing, burglary, theft, robbery, theft of motor vehicle, etc.

Officers need to know and understand relevant laws before they can assess and counter threats.

Other laws, such as smoking ordinances and Americans with Disabilities Act (ADA) that officers may need to enforce, are listed here. All of this section applies to the small operation.

Emergency Procedures—Section 7

Employee procedures in the event of an emergency. Security response is obviously different from other departments.

Each type of emergency (fire, accidents, illnesses, active shooters, earthquakes, etc.) is listed with the appropriate departmental response. This section may be a separate manual which is distributed to all departments. Include it in the manual anyway.

Incident Response—Section 8

The procedures for how security officers handle all non-emergency incidents on the property are outlined here. These may include intoxicated persons, panhandlers, sleepers, water leaks, property damage, etc.

Everything from first response to investigation and report should be outlined.

Documentation—Section 9

Documentation is what Security is all about and here is where it is all explained. Procedures for writing incident reports, daily logs, and other reports are included.

Also, list your rules for records retention, the revisions of the security manual, etc.

This is a somewhat generic outline. If you have a pool or a nightclub, you can add them. If you run a bed-and-breakfast, or an amusement park, or some other destination, keep the same format, but customize it to fit your property.

If you are not sure what content to include (Like a Use of Force Policy), fear not. This book covers everything that I think a manual should include. Also, if you are not into my numbering system, use your own or don’t use one. It is not expected or required.

WRITING THE MANUAL

Now that we have an outline, all we have to do is fill it in to create some content. Here is an example of a “page” in your manual.

3.3.5 Breaks

The Security Department provides three breaks for a normal 8- or 10-hour shift. Officers are paid for break time. The company believes all employees should have rest and nutrition periods during their shift.

- First Break is 15 minutes
- Lunch Break is 30 minutes
- Second Break is 15 minutes
- Breaks can be combined (i.e., two 30-minute breaks) at the supervisor’s discretion
- Since break time is paid time, breaks will be taken on property, on-duty, in uniform and available for emergencies.
- If an urgent need for a security officer arises during a break, the officer will respond and re-start their break upon return.

- Officers not able to take their break due to an emergency will be compensated at the time clock for that number of minutes lost.
- The above procedure is not intended for refusal of breaks to receive compensation.
- Breaks will be taken in designated areas only.
- Supervisors will approve all modifications to break times and ensure that each employee receives their breaks.

The above textbox has an example of a completed “page” of the manual. Take each subheading in the outline and make it a title of that page. The first paragraph is a summary explanation of the procedures: why the policy exists, what it protects, its background, etc. Then each subsequent paragraph or “bullet point” is one procedure or rule for that heading.

In the example, Breaks is the subheading and begins a new page in the manual. Note the numbering system used allows you to add and remove procedures without changing every consecutive number. After the heading, a short paragraph explains what the policy is and why it is important.

After the opening paragraph, each rule is listed separately with one or two brief sentences until all procedures for Breaks are covered. Note that the format is important in that it follows the outline and is consistent across all sections.

Break policies (and many others) had largely been verbal ones until officers at several major hotels filed a class-action lawsuit to be recompensed for lost wages. They were required to come to work 15 minutes before their shift for a briefing without clocking in early. The additional time would be added on to their lunch. One of their claims was that they were technically “working” while attending the pre-shift briefing, and not being paid for it, which is apparently a no-no. The other claim was that even though the lunch was extended, they rarely got to take the entire break due to “emergencies.”

The hotels and the security officers came to a settlement where the officers received back-pay for the estimated hours they were not paid.

I was deposed for this case as a new director and learned a great deal: (1) do not inherit someone else’s policy manual without reading it; (2) do not assume that “everyone knows the policy” is accurate; (3) make policies such as this one clear and specific so that it will be followed consistently; (4) never let an employee work off-the clock, even if it is voluntary; and (5) this is when I learned to write my own policies that I could defend in a deposition. The one in this chapter on breaks is very similar to one I wrote after that case.

Other Sources

Without a doubt, you do not have time to write a few hundred manual pages as described previously. Nobody expects you to do that because you are a director. So let’s get some help, and we will direct them. Start by looking at your outline and see what information has already been written for you.

The Human Resources Department probably already has policies such as Sexual Harassment and Confidentiality in written form. See if you can get the electronic version so that you can format it the same as your manual.

If there is a company manual or corporate manual, these documents may also contain some of the generic policies you want.

You have saved all of those policy memos for a reason. Now is the time to pull them out and convert them to policy. I hope that it is just a matter of changing the format.

Note: This is a good time to mention that inserting photocopies of memos or policies into your manual looks bad. Even if you do not care about looks, the photocopies make it look spontaneous, outdated and poorly executed. Take some time and do it right. Retyping a page does not take that long.

If you have another department that is on the ball, it may also have these policies written for their folks and would be happy to share them with you. For example, the Food and Beverage Department may have a conduct policy that you can borrow or from which you can at least get some ideas. This lends consistency to all departments if everyone is using similar policies.

Finally, many of these generic policies are available on the Internet. Do not plagiarize—except from me because that is why I wrote this. Make sure you have permission or make drastic changes if you use someone else's work. As you gather written pages, cross them off your outline to show your progress.

Delegation

The next step is to delegate some of the writing. Your supervisors and managers can do much of it. If they shy away, it is because they are lazy or lack confidence, not because they are incompetent. This is barely different from writing incident reports, which they should be particularly good at if they are in positions of leadership. You may even have some above-average officers that are up to this task.

Start with your outline and go through it, assigning sections to your list of delegates. Give each of them five sections or pages to write. They can choose the ones they want, or you can assign them based on where you think their interests or experiences fall. As you assign them, make sure they have the format and a deadline.

You can email them a sample, such as the one we wrote previously on "Breaks" and allow them to cut and paste their paragraphs into your format. If their format does not match yours perfectly, accept it, congratulate them for a job well done, and then modify it to make it consistent with yours.

Make sure you give them a deadline. The deadline should be reasonable because they do have other things to do, and you do not expect them to do all of it at home. Perhaps two or three workdays per section are adequate for most. Most will not object to the idea of writing policy, but are more likely to freak out about writing anything. Unfortunately, our employees do not come out of high school with an ability to write a paragraph. I am a bit more tolerant of this than I was before. People are embarrassed about their writing, but this can be used as some learning and not a tipping point in their career. If composition is not their strong point, teach them if you can, or accept less if you must. More on this topic in "Hiring."

You also may find some people in other departments willing to write policy for you. Those who enjoy writing—and there are a few of us—will do it with a smile.

Compiling

As you start to receive everyone's homework assignment, it is time to get organized. You can print the pages and start sorting them by section using the outline as your Table of Contents. You also can do this in your word processor by naming each section as its own file using the numbers as the naming convention. This way, they will be in order in your computer and missing entries will be easy to spot.

Once the manual is complete, you can print it out and compile it into a three-ring binder. If you want to save paper and you have the resources, save it to a PDF or some other form that cannot be edited. You do not want anyone making unauthorized changes. Make sure you have several backups on different servers and media.

Updates

The manual can, and should, change often. The property changes, management style changes, and local laws and procedures change. Try to avoid stuffing memos into a book and expecting anyone to understand your intent or take it seriously. In a hard copy, remove the outdated page and replace it with a new one that has the revision date on it.

Save the old policies, even if they were a mistake or irrelevant now. If you have to defend a policy that was in place when an incident occurred, you need to have it available. I suggest filing these old polices in a binder in their same order and note the effective date and the replacement date.

Summary

The manual for your department serves several purposes. First and foremost, it assures consistency (if it is followed by everyone). Second, it provides a central storehouse for all the rules so one does not have to go fishing through old emails or memos to find a policy. Third, it is the reference for discipline. If someone is late five times in a month, there should be a policy in the manual that defines the discipline for that offense clearly. Finally, it will be used in just about every lawsuit regarding security.

As I learned the hard way, the manual can work against you if it is not written well and kept current. If you go to court with a manual that is incomplete, out-of-date and inaccurate, you will be asked to defend it which is difficult at best and costly to you and your team. On the other hand, if you have policies that put safety first (when applicable), are proven practices that are current, comprehensive in scope, it is difficult for the opposing party to accuse you of taking shortcuts or ignoring risks. If you struggle with this important piece of your system, get some help. Procrastinating will only come back to bite you.

Your manual will accompany you to your first deposition. Your integrity increases when you are prepared. An organized, complete, and current manual shows everyone how confident you are.

EMERGENCY MANUAL

Emergency procedures and response are covered in Chapter 5, so we will not argue procedures here, but will discuss how to write them. The emergency procedures manual is actually a controversial issue in most Security Departments. Most directors can find many more reasons not to have one.

First, we do not want to take the time to write one. Second, writing one will probably make us aware how unprepared we really are for most emergencies. Third, and most compelling, is, “Why should we create a book that will sit on a shelf and become outdated?” We will not have the time or the presence of mind to refer to it during an earthquake or fire anyway. Sound familiar? This is explained in Chapter 5, so either read that now, or take my word for it and let’s write this manual.

Make sure we are clear that the emergency procedures manual is for the response to emergencies and does not include business continuity, continuity of operations, or any of the stuff that happens *after* the emergency is over. This manual will cover procedures that save lives and property. Once again, think about explaining why you have a manual that explains Lost and Found, but not one for evacuating the hotel.

Hazards and Threats

Before we can write procedures, we need to know what our potential emergencies are. Yes, we did some of this in Chapter 1 for the Risk Assessment. Not every emergency was listed there, but those are a good start. Add to that list any other hazard or threat to life or property that can happen at your facility. I like to separate them into “Natural” (Hazards), “Man-made” (Threats), and Technical (servers, power).

One of the worst events I had at a hotel was a power failure on Thanksgiving night. The power went out regionally for a few hours. The data servers did not survive the power bump and their back-ups…well, let’s just say someone somewhere is not going to list that job on their resume. Anyway, we had back-up-power but the systems that ran cash registers, hotel check-in and keys, and just about everything was toast. On a holiday, it is often hard to get people that know what they are doing off the ski slopes, but we finally did after one of the biggest revenue weekends was lost.

I always say that a false alarm is good training. This was kind of the same thing in that we found where our data vulnerabilities were and how reliant we were on them. This is a good exercise for all departments to enable back-ups and learn how to operate manually.

Natural emergencies are weather-related events like hurricanes, tornadoes, floods, and blizzards. Earthquakes, lightning strikes, and “Acts of Nature” are also included. If you live in the mountains, you can probably exclude hurricanes, and so forth.

Man-made threats make up most of our emergencies. Fire, active shooter, bomb threat, explosion, gas leak, bioterrorism, robbery, medical emergency, drowning, and vehicle crashes are some of the incidents you might include on this list.

Technical emergencies are not always emergencies and do not always involve security, but there are some for this list. Power failure, server failure, electrocution, elevator and escalator mishaps, and other machine malfunctions may be emergencies that require a security response.

Starting the Emergency Manual

This manual can follow a similar format as the security manual, but it needs to be simple, easy to read, and succinct. We are not going to add a lot of narrative and extra stuff. This is our nuts-and-bolts manual used in emergencies, so stick to the necessary facts. The simplest layout for this manual is to make each chapter a different emergency procedure. Having already determined what those emergencies are, create your outline by listing those events: fire, earthquake, power failure, active shooter, etc.

Some emergency response measures are common to many different emergencies. Evacuation is one that is used for a majority of incidents. Evacuation procedures will be their own section in our manual.

Under each heading (each emergency event) list the steps to be taken and by whom. You may find it easier to list responsibilities by department or position. Security Officers do A, B, and C. Engineers do X, Y, and Z. Bell persons do 1, 2, and 3. Once you have worked this out, your manual is essentially finished.

Testing the Manual

You are not finished! The biggest mistake planners make is printing up a well-written manual and placing it on a shelf in their office. Some go an extra step and send one to every department and feel satisfied. You have heard the problems with this many times. First, you are not going to remember what the manual says a year later when an earthquake hits. Second, nobody you send it to will ever read it. Third, departments change, management changes, and the building changes so the manual must live and breathe.

Most importantly, the testing and updating of the manual are necessary. See Chapter 7 for emergency planning processes. This is how the content of the manual is tested and upgraded. Your manual, if used in this manner, will never sit on the shelf and collect dust. Everyone will already know what is in it.

INCIDENT ACTION PLAN

An incident action plan (IAP) is a document used in preparation for a special event. As in most planning processes, the collaboration and communication prior to the event is more important than the document itself. An IAP differs from emergency planning because it prepares for a scheduled event. IAPs are commonly used by your police, Fire and Emergency response agencies to plan festivals, parades, and even events at your hotel or amusement park.

In an ideal world, the private sector would get together with the police lieutenant or fire chief when they do their planning so that everyone is on the same page. Another way to do it is to exchange plans so you know what the first responders are doing. They have different responsibilities during an event, but there is some overlap and there is certainly a reason to know each other's hands.

Whether you work with your local government or not, you need to get together with other departments at your hotel. Hopefully you are doing this already in the form of a "pre-con" meeting or events meeting. An Incident Action Plan, for the purposes of our private enterprise, does not only include emergency response, but it may include less dramatic things like how the trash is removed, parking considerations, and how money is handled. Rather than provide a template, I will hope that you either use whatever your local Incident Commander is using or make something that meets the needs of your property. However, here are some suggestions for items to consider in your Incident Action Plan.

Incident Overview: This is the name of the incident and a brief summary of what it is, who is sponsoring it, and its purpose, for example, "New Year's Eve fireworks and party for hotel guests sponsored by the Marketing Department." Included here are estimated attendance numbers, staff numbers, and other departments involved.

Location: The location of the event, including all convention rooms, lobby, offices, etc.

Date/Time: Date or date range of the event including start and ending times.

Workforce-Management: List each rank beginning with the Incident Commander, their title, and name of person assigned.

Workforce-Posts: List each post, its location, primary duty, and person assigned. Note that we avoid the shotgun approach of putting 10 officers on the perimeter. Each officer needs a post and post duties, even if they overlap. Posts might include dispatcher, door host, perimeter bike rover, etc.

Special Assignments: This includes outside companies like ambulance services, police, and other contractors. Also, include your own people that have special assignments like undercover, investigators, etc.

Special Procedures: List only those procedures that are not normal for your property. In other words, do not list fire evacuations, as those procedures do not change. But you may include riot, crowd control, missing children, special money drops, or whatever is relevant to this type of event.

Other Department Procedures: List those responsibilities of other departments relative to this event. Perhaps Engineering has a Fire Watch on the roof for a fireworks show, Marketing is responsible for posting certain security signs, and Housekeeping cleans up empty glass containers for safety reasons.

Miscellaneous: You can customize this template however you want and add to it those sections that meet your company's needs.

Use the IAP so that everyone, including your supervisors, dispatchers, other departments, and even police and fire departments know how to manage the incident and what you will be doing for contingencies. My favorite use of this form, next to the benefits of getting everyone together to plan, is to have it for next time. Imagine the IAP for the Route 91 Harvest Festival in 2017. You can bet that was scrutinized on October 2 by a few hundred government officials, lawyers, risk managers, and CEOs.

A hotel sponsored an annual festival where streets were blocked and about 5,000 people attended, enjoying food, craft sales, and entertainment. A drunk driver who was completely disoriented and trying to elude police, busted through several barricades, and headed into the center of the festival. It so happened that the police were guarding those barricades and as soon as he passed the last one, he was shot several times until the vehicle stopped.

The crowd responded by running away from the shots in all directions. Many people ran into the adjacent hotel and their screams indicated there was an active shooter. The crowd outside was seeking cover indoors, while the people indoors, who thought there was an indoor threat, ran outside. This caused chaos and many injuries from the panic. The only one injured, killed actually, was the drunk driver. Lesson number one: It was not an actual active shooter—just the police shooting a bad guy. Lesson two: The panic seems to be worse than the event in many circumstances. This is difficult to plan, but all possibilities should be considered.

3

Training

Some companies, no, most companies, well just about all companies fudge on their training. That's not just security, but housekeeping, food service, maintenance, and the rest. I suppose we have two reasons: Time and money. By the time you get someone hired, you are generally under pressure at having an open position, working someone else too hard to cover, and you have a noticeable gap in service. Most of all, training is expensive. Most of us don't budget for it, and if we do, we do not accurately predict that Brian will quit before the holiday weekend. The result is that the new guy gets hired on Friday, and by Monday he has experienced enough to call it all good.

Horse Hockey! We cannot compromise on training! It can threaten life safety and cost you big money. It is bad for business and will ruin you as a manager.

In this chapter, I will first make the case for having adequate training—superior training if you do it correctly. Then I will help with the financial side and the executive buy-in. So, if you turned to this chapter by mistake, you have come to the right place. Get some popcorn and stand by.

MAKING THE CASE FOR TRAINING

There are three major reasons you need an effective training program. There are more like a hundred reasons, but I narrow them down here, and I always do that in threes.

Ability

This is a huge category because it includes capabilities of your employees, wisdom, experience, common sense (if it still exists) and accountability. (Those 14 letters could change your department right now.)

I have observed over the years that in the absence of training, a security officer will revert to his/her prior experiences. In the absence of prior experience or training, the only option is primal instinct—or fight or flight. Let's review these in reverse order.

Fight or Flight. Most living species have this primitive instinct. When confronted with a threat, the brain makes a decision: attack; aggression; or to get the heck out. You can

DOI: 10.4324/9781003037644-3

see this with dogs, bugs, small children, just about every animal either has a positive defense mechanism or they know how to retreat very quickly. Your completely untrained security officer, who you hire right out of high school with straight As and president of the chess club, if confronted by someone violent, will likely freeze as they consider their options, and when they realize they don't have any, they will likely run away or get their butt kicked. Look at videos of active shooters. You can tell the victims that have not had active shooter awareness training. They pause, waste precious seconds deciding what they should do, then hide because it's too late to run. As long as we do not ignore this, we can work much better with a clean canvas than try to make a Renoir from a Picasso. The entirely untrained can be our best trainees as they have no preconceptions that we need to overcome.

Prior training. A security officer who has received some sort of prior training, whether it's military, police, corrections, or other security companies, must be re-trained (sorry folks). That means we have to overwrite everything they know. This is difficult, as that requires time and repetition. For example, suppose you hire a bouncer from a local bar to be a security officer. There is no way he had training provided by the corner bar, but he is large and was a wrestler in high school. It does not matter that you train him how to de-escalate and walk someone out, because, as a last resort—he will tackle his opponent (or chokehold or whatever) every time. To overcome this old muscle memory, you must make new memories and that requires more than one-time training or following someone around.

Do not take the term "muscle memory" too literally, as muscles do not have memory—or do they? While some physicians and athletes might argue that muscle cells, that regenerate when working out, have the "memory" of doing whatever it is they were doing, in this case I am referring to patterns of activity in the brain—habits.

Muscle memory, the way I teach it, is simply learning a pattern until it becomes part of your memory and automatic. A simple example is a typist. (Alas, I wrote this entire book with two fingers.) Your fingers learn the location of the keys and type the words without thinking—or so it seems. Remember that drive home last month when you were trying to think of an excuse to tell your spouse why you were late? Suddenly you are in the driveway without any recollection of your drive home. That is muscle memory. When we train anything, we repeat, repeat, repeat until it becomes second nature. That means in addition to the initial training, there needs to be follow-up in the form of in-service training. We will talk about repetition more throughout this chapter.

Consistency

Most managers look at this linearly rather than in three dimensions. Once you get a training program just the way you want it, you teach it to Bob. Bob teaches it to Roy, who teaches Mary, who teaches Fred. Great. We have taught our methods across the entire team. Then we need to teach the next batch of recruits, so Bob, Roy, and Mary teach Danny, Lanny, and Fanny. But wait. Mary and Fred and their co-workers need in-service or refresher training, so their training is current and consistent. That must be passed across and down. Then the policy changes and we have to re-train everyone across and down.

It gets complicated and begs for someone to keep it organized, on track, and consistent. Example: suppose you have a policy of no persons allowed in the hotel without a room key. The new spa opens and the policy changes to allow persons with reservations at the spa to access the elevator to go to the spa. Goofus, who works early morning and never sees a manager, stops the CEO's nephew from accessing the gym at 0500 and embarrasses him. I use that as a simple example because it happened to me (author laughs out loud). But consider a critical policy like "no weapons allowed" or anything involving use of force. If Goofus has not been trained on the new policy, it could get contentious or even dangerous.

To repeat, we want everyone to have the same training so that tasks are performed within policy and to our standards. The old days of putting the new guy with whomever is around (the shadow method) does not allude itself to consistent training. Unless there is consistency, among the trainers, everyone will train the way they have always done it and soon your department will evolve—literally—to something you do not recognize. The training manual, if written and used effectively will resolve these disparities.

Another way of looking at this is to look at your objectives. Your objectives are probably: Everyone will perform tasks like I do; Everyone will learn the tasks the way I learned them; and since my staff represents me and the company, I want them to do the tasks the same. Working back from your objective will make the training and policy manuals right themselves and ensure that your department is professional and efficient.

In security, we must be consistent in the way we write reports, greet guests, patrol certain areas, use force, and so on. The word-of-mouth training program will not work for these important tasks. Consistency becomes even more important as we get into risk, which is in the next section and throughout this chapter.

Liability

Let me start my description of liability with this important anecdote. As you may know, most lawsuits regarding security will accuse your company of inadequate training. As one who has worked both sides of these cases, I rarely find a training program that is adequate. My company was sued once for a violent incident between two guests. The assertion was that we had inadequate security, inadequate training, negligent this and negligent that. When the discovery process called for the training files for all my security officers, it was the moment I had prepared for all my career. My training manager photocopied every page of every file and filled four bankers' boxes! Our attorney called one day to see how we were doing on this project and I told her we had four boxes for her. The opposing attorney found out and immediately withdrew the charge of inadequate training. I will outline the training program you want to have to protect your company from these claims.

Inadequate training hits you twice. First, it means your staff is not doing things the way you wanted, nor reducing liability and costs to the department. Second, if your training is inadequate, you are going to lose that aspect of a lawsuit because you will either have no documentation, or whatever is documented will be different from officer to officer.

Many cases have been lost because training was not documented. The plaintiff will find a former security officer that you do not even remember, find out that his training file does not exist, and ask him simple questions like, "how many hours of Use-of-Force" training did you have?" "I don't know." Well, what did they teach you? "Ummm take downs, how to unlock handcuffs, and wrist lock." Ok, when you broke my client's arm applying the handcuffs, were you following the training, or you don't remember?

Believe me, you would much rather have a documented training file that he can use to refresh his memory when questioned. Mistakes and accidents during force incidents are one thing that we can deal with, but an officer who seemingly ignores training and does something on his own, is YOUR fault. This is called inadequate or negligent training. Not to worry: Our training will not be like that. (How is your popcorn?)

Using all three components of training puts you in a better position when defending the actions of your folks. It will not prevent a bad incident, but it will be less likely to happen, and you will be better prepared to defend it.

If you rely on a contract security company to provide their own personnel with their own training, stick around, because you still need to make sure they have adequate training.

FUNDING TRAINING

Training is going to be the foundation of your department. It is also the biggest expense in hospitality security and the hardest to sell because it is perceived to offer little or no return on investment. Remember, here in the private sector we must justify expenses as necessary for the operation of the business or as a revenue generator. Our executives in the C-suite do not necessarily understand training for its own sake, or costly training programs. Fortunately, there are ways to articulate the need for training, its advantage to the business, and even its return on investment.

Professionally trained security officers save the company money. (Make that the title of your next training proposal.)

Guest Safety

The obvious first choice is guest safety. The security dilemma has always been justifying our existence because it is difficult to prove a negative (fewer incidents with security than without). Most experienced executives do not need to be shown the metrics of this equation because they know the effect of visible security. However, it can be done. One way is to study another property that went from nothing to having visible security and note the improvements (or the opposite). Another way is to accumulate positive guest comments and show those that praise the presence of security.

Guest Safety in my opinion includes the guest's feeling of comfort. Do they feel safe on your property? Many surveys answer this question by asking guests if they had any reason to call security during their stay and if their issue was positively resolved. Other questions are "did you see uniformed security officers during your stay?" And "Did you feel safe in your room and when traveling around the property?" Of course, security needs to hold up their end by being effective, friendly, and visible. One tactic I used was to post an officer or two at the lobby during peak check-out times. I thought it would help put security at top of mind before they worked on their survey. This may seem like "trickle-down feelings of safety" because it takes a while to get enough positive responses and to show a marked improvement in perception, but it will happen.

Liability

An able officer can reduce and prevent exposure to legal action. An officer who is poorly trained and gets into a situation where he uses force, will likely defer, as we mentioned before, to whatever else is rattling around in his brain. An extreme example of this is a hotel I knew that hired Tongans to supplement security on holidays and special events. (Tonga is a Pacific Island nation whose natives are generally large and most intimidating.) Because the director there knew of the dangers of having untrained officers, these guys were given strict instructions to "Observe and report," "Don't touch anyone."

After two weeks or so of work, when everyone was starting to get comfortable with him, one of the men was ejecting an older man from the property. The older man was homeless, walked with a cane, and was refusing to leave. The officer grabbed his cane and started beating him with it all the way out the door. The homeless man filed a battery report with the police, but fortunately did not get a lawyer. This was inadequate training, excessive force, aggravated assault, plus whatever injuries there were. And it's all the fault of the hotel.

This is a selling-point for training. Defending allegations of excessive force is awfully expensive, even if you are in the right. Your money-handler knows that already. That person may say something like, just tell them how to do it right so there are no problems. Your argument is in the upcoming pages of this book. Training is not a "read-and-sign" memo. It is repetitive reprograming of the mind to lose those old habits.

Another argument from your money person may be to just contract it out. I agree that sometimes this is the better option, but it does not mean that liability ends. Your contract security company—if they have a contract at all—likely has a clause that says something like, we are not liable unless there is negligence on the part of the guard company. OK. Who decides that? Yes, a court of law. So back to the original problem. How much will it cost to defend this allegation? We refer back to rule number one, which is training—even if it is an outside company.

As we progress through the upcoming pages and chapters, you will get an idea how training saves money. I can promise you that whether you have proprietary or contract security, that the more training you have, the more successful your department will be. (That means saving on claims.)

TRAINING CULTURE

Two of the types of security officer you will employ are: (1) I am here to get a paycheck and possibly too dumb or lazy to do anything else; and (2) I really dig the prestige, helping people, and getting a little action. (By action, I mean catching bad guys.) Each of these types of officer requires training—especially if you want to keep them.

I found that building a "training culture" saved money, reduced turnover, and increased morale. The days of the shadow are gone, my friends. No longer can you hire someone, put him with the senior officer, and hope for the best. This is not productive training. The "new guy" either learns nothing, or a bunch of bad habits; or he learns all about dayshift, then goes to the grave and encounters a bunch of weird stuff that only happens in hotels and creates a liability for you.

The training culture centers all the activities of the security department around training. Though it takes a while to build, the training culture will pay off big-time once it is set. Here is my recipe for a great training program.

Training Manager

The qualities of an ideal training manager are: She loves to teach; He is engaged, or otherwise loyal to the company and the concept of "security." She is organized and documents everything. He is creative.

Though you probably will not find someone with all those qualities in your organization, find the most that you can. If your new training person does not have those qualities, we will have to delegate them, because they are each vital. Notice I said "promote" instead of hire. Bringing someone from outside to build your culture will be difficult. She will not have the trust, the experience, and the culture that you have built. Promoting from within is always preferred anyway. Also note that I call her a training "manager" and not a coordinator, or supervisor, or "guy" or "dude." The training manager needs to be a symbol that you are taking this stuff seriously. He needs the ability to hire, fire, and discipline. He needs to be able to boss people around, because there will be plenty of that coming.

If you are unable to find this golden child in your realm, find one that has the love, the engagement, the loyalty, the creativity to build her program. In a word, find the passion. This program is starting to get exciting. I can feel the heat already.

Unique Classes

When I was a fledgling officer, just getting my start in a big hotel casino, there was a guy who offered his "academy" to the various casinos, and we had to sit through his class for a week. If you have ever taken a driver training class, you know how horrible this was. Of course, he had to include certain things that were not exciting, but my gosh, I forgot everything that I learned for sure.

I will show you later what topics you need, but include some things that you do not know that you need. My team was partially armed, which does not mean they had one arm, but that some of them carried guns. It was easy to come up with classes that were fun, physical, and enlightening. But even so, there are things a security officer needs to know, besides verbal karate—or whatever it is called.

This is where the creativity and passion come in.

Include Everyone in the Process

I had a boss once who told us regularly, "You guys may be smarter than me, but I am in the driver's seat." This was not said with arrogance, but as a matter of fact. He was in charge and that was it. This gave us hope and possibilities, because he was not the all-knowing, untouchable leader of whose flatulence we were not worthy of smelling. Rather, he just got there first, and we had the same chance—just as soon as he died or something (the author laughs at his own pity).

I vowed to take this same sense of motivation and translate it to my troops. When you remove your bias and your preconceived notions of someone's abilities, you find that just about anyone can do this job—our job: the one in charge. So, I train everyone as if they will have my job one day. They may not want it or be ready for it, but if you open your mind to everyone, the cream will rise much quicker and suddenly you have a talented team.

Continue the Training from Day One until the End of Time

We can save money on attrition in two ways with a good training program. The first way is to use the initial training as the observation period for your new officer. Putting an officer right into his duties on the first or second day does not give you a chance to watch his interactions, behavior, and other opportunities he has that could put you in a position of risk. A substantial training period will give you a chance to model correct behavior with a qualified officer, and to observe poor attitude, violent behaviors, and learning types. If you have to let an employee go, it is better and cheaper to do it in the first few days during training than to wait for months until you actually observe a costly mistake.

The second and more positive way to prevent turnover is by producing qualified, professional, confident officers. These employees historically take more pride in their job and company, produce more, and are thereby more honest and likely to stay longer.

Frankly, the job of a security officer is boring most of the time. I believe that if you keep your troops engaged, they will stay longer, learn more, and be more loyal. One way to do this is constant training. Most of them will look forward to it if it is done right. Besides training, there are some other ways to earn engagement and those will be revealed later.

QUALITY IN IS QUALITY OUT

You would not hire a cook who never worked in a kitchen, and even if she had experience, you would have to teach her how to use your kitchen equipment, the menu options, ingredients to all of your signature dishes, and how they are displayed on the plate. The same goes for the guy who repairs your air conditioning and drives your shuttle. Whether you manufacture widgets or provide a service, the better-trained worker makes a better product in less time. In security, our product is protection of assets, and in hospitality security, we add guest service as a product. A better-trained officer is going to excel at both, identifying problems before they occur, preventing criminal behavior, and greeting guests with confidence and professionalism. Protection of assets and superior guest service will come naturally when training is in your culture.

When security officers escorted some unruly guests from a private party at a hotel in 2010, one of the guest's friends started a fight with Security to get them to release his friend. A struggle ensued and the original offending guest was struck by one officer with a bottle. The injured guest sued the hotel for negligent hiring, training, and retention because the officers did not know how to handle intoxicated patrons. The court sided with the plaintiffs after a security expert explained that proper background checks and training relevant to their jobs would have prevented the officers from losing control.

Too often, "bouncers" are hired more for their appearance and size rather than their training or expertise. Make sure the hiring and training process is relevant to the skills required to perform this particular job. Guest relations, use of force, and de-escalation techniques are training programs often overlooked, but are necessary in any hospitality security program.

It is tempting and sometimes seems necessary to fill the open position with someone as soon as possible. Establish your training program and stick with it as if you have no other choice. It is just a cost of doing business. Your business will have proven positive success because of a more professional, better-trained security force.

Previously, I mentioned that skills can be taught but attitude cannot. It is a common mistake to hire for experience and hope to save money by not having to train someone who was trained elsewhere. This may or may not work out for you, but you need to weigh this risk and decide if it will work in your favor. A police or corrections officer may be able to effectively arrest bad guys, but have they ever had to worry about making a false arrest? When they learned to quell riots, did they get training on dealing with a bunch of drunken conventioneers? Maybe you will get lucky, but you cannot design your training program around luck. Documentation and consistency are the two keys to training, and the previous examples will not satisfy either.

CONSISTENCY

In the previous section, we talked about the importance of training for reducing risk. Even though risk was used as the justification for selling the program to your boss, it is the absolute primary reason that you have to provide training. This training, whatever it is, must be applied consistently across the entire staff. If two officers receive different amounts or types of training, you may be found negligent when one takes a different action than the other.

This is also why we cannot rely on an officer's prior training as being adequate for our hotel. If all of the hotels in your community used the same training program, then that gets you part of the way there. But there are still policies and procedures unique to each hotel that would require consistent training by the hotel. This especially applies to contract security if used at your hotel. Make sure they receive basic training from their company, but also ensure they have specific, consistent training on your hotel's practices and techniques.

TRAINING PROGRAM

We have established why training is important: Ability. We then explained the importance of Consistency. Finally, we determined that its cost can be justified: Liability. Next is the implementation of your program.

As discussed earlier, training is a full-time job. Therefore, our first step is to fill the position of Training Manager. This person will write and present various training programs, evaluate trainees, coordinate the timing and schedule of the different training programs, and maintain the records of all of it. Besides being able to do all those things, you will need someone who understands learning and teaching styles and techniques and who can develop and modify training programs as policies change. In addition, this person should be able to monitor and research current events and case law while keeping abreast of how risk is managed within the company.

Finding one person adept at all these skills is difficult, if not impossible. Well, almost impossible because I found one. But if you cannot, divide those skills. If one person can keep track of all your training and even decide what to present, but does not teach well, then find a teacher. You get the idea, but please do not compromise on any of those prerequisites.

Training Components

While most training is covered in a classroom setting, we need Field Training (I called it Floor Training because we had no field) to practice what we learned in class. The third component is in-service training which allows for updates and repetition.

All three components are necessary for a successful security department that reduces liability while protecting assets.

Classroom

You should never put an officer into service without a minimal amount of orientation to their new job, the company's policies, and relevant laws. Much of this can be taught in a classroom setting. Many security companies choose to contract this service. There may be someone in your area that can teach security basics for all of the hotels or other security functions in town. Whoever teaches at your academy should have some teaching skills. We used an instructor development class which was taught by some law enforcement trainers. You absolutely do not need cops to teach you how to teach, but in my case, they taught the field training as well, which is a bit more specific.

A search for "Instructor development training" will yield many results. Beware of websites that are named "government" or POST or something official. If you want government training, look for ".gov" on the site. Instructor Development training does not teach you what to teach, they teach you how to teach. There are different learning styles, such as visual, auditory, and kinetic. Individuals learn in different ways and at varying speeds. Once you know what to look for, it is easy to modify your training for your audience and increase absorption.

Classroom training should use various media and learning platforms.

- PowerPoint® is an effective method that is widely used, but if it is presented poorly, it will be worthless. Use lots of photos, less words, and uncrowded slides. Tell stories. Personal examples of a situation are memorable and interesting.
- Engage the audience to tell their own stories, ask questions, and participate.
- Videos are interesting and explanatory—if used in moderation.
- Play recordings of phone calls or radio transmissions.
- Use guest speakers—bring in a police officer or a department head or even a fellow officer to present a portion of the lessons. This adds credibility and is memorable.
- Role-playing is not an option. It is required. You can explain and talk about topics like de-escalation, but until it is practiced, it will not be absorbed.
- Exercises just like in high school are used for a reason. Participation and retention escalate when you get your audience working.
- Testing honestly freaks some people out—to the extent that you might lose an otherwise good employee. I recommend testing to determine retention, but also to evaluate how good the class and the instructor are. If someone cannot handle a test, there are other options. Be flexible.

If you are going to introduce an academy to your existing training program, work out a schedule to put all officers through it. The veterans can be put in class with the rookies at a pace that does not tax your staffing levels. Consistency and documentation are the names of the game in training, so you want everyone to go through the same training.

Training Objective

Well, we cannot start training without a syllabus. That requires some objectives (remember we always work backward from our goals). Your objectives may vary, but there are some basics that you cannot omit.

Security job description
Laws of arrest
Physical arrests (defensive tactics)
Use of force
Practical training (role playing)
CPR, first aid, AED
Emergency response
Guest service
De-escalation skills
Investigations
Report-writing
Company policies
Department policies—conduct, appearance
Cultural awareness
Hotel and other procedures

Risk management
ADA, sex harassment and other federal
Property-specific policies
Property-specific venues (nightclubs, retail, restaurants, pool, etc.)

Security Job Description is the orientation to the job. What does an XYZ hotel security officer do? Besides keeping everyone safe and protecting assets there are some other expectations that need to be introduced. Patrol of the parking lot, lifeguard at the pool, checking IDs at the bar, Casino, theme park, shopping mall, airport transportation, and on and on.

Basic Laws

You may be surprised at your new employee's perception of what her authority is. You need to start at the beginning with the definition of a crime, the elements of common crimes found at your hotel, misdemeanors vs. felonies, grand theft vs. petty theft, etc. Check your state laws because some states give the security officer the same arrest powers as a police officer and some limit them severely. There are all sorts of laws in between the two extremes. Most states will require the officer to witness the crime to make an arrest. I do not know of any state that allows a private person (which is what security officers are) to make an arrest on behalf of another person (i.e., he stole my purse).

Each law needs to be reviewed as to its elements. Elements of a crime are those facts that must be included in order to charge someone with violating it and arrest them for it. For example, depending on which state, the elements of petty (or petit) theft are: (1) taking the property of another, (2) with the intent to deprive the person of the property, and (3) where the value is below $500. Intent is an element of most crimes, but not all. If you saw someone put a candy bar in their pocket and walk around the store, you cannot arrest them until you know their intent was to keep it. They might have changed their mind and bought a bag of chips if you had not deprived them of their liberty. Same goes for trespassing, which will be discussed in detail later. You cannot arrest someone for trespassing if they are heading toward an exit. Well, you can but you will have to convince the police and if that works, to a judge, and if that works, to a lawyer when he sues you for false imprisonment, slander, libel, inadequate training, negligent retention, and whatever else they can find.

Laws of Arrest

In some states, the police are required to intervene and make an arrest whether they want to or not. We have the luxury of being "non-sworn." We do not take an oath to uphold the laws of the state, and we do not have qualified immunity like a police officer, so an arrest is the last resort for us. Contrary to popular belief, we are not required to arrest for domestic battery, child abuse, or any felonies. Again, please check your jurisdiction and get some training for yourself if you are not familiar with these laws.

Do not spend a lot of training time on laws that are not often encountered in a hotel. The serious ones like murder, arson, rape, and kidnaping are pretty self-explanatory and if an officer witnesses something like that, there is almost no bad decision to make. Knowing the difference between third-degree manslaughter and first-degree homicide does not matter if you witness a stabbing. Hold the bad guy and call the police.

If you are reading this thinking that your company policy is "hands off" observe and report or something similar, there are going to be situations where an officer must intervene, so they need to know what action is prudent. I am reminded of a video circulating years ago of two security guards watching some gang members beat up a lone female. They stood and watched, while waiting for the police. They followed their policy, but the girl suffered serious injuries and the guard company was ridiculed and could have been sued as well.

Search and Seizure

Our Constitution protects all of us from illegal search and seizure. We, as citizens do not have any rights over our fellow citizens, so these are topics that must be trained to avoid illegal searches. What I often see is a security officer making an arrest and either failing to search for weapons or searching and removing everything from the arrestee. The correct method is in between those two extremes. When security searches someone, it must be: (1) subsequent to an arrest (stop and frisk does not apply to us) and (2) for our safety only. We do not search for drugs or contraband or even ID. A voluntary search is not recommended either because how can someone volunteer their constitutional rights away when they are in handcuffs surrounded by their fellow citizens who have no authority to do so. Make sure they do not have weapons and that is all. If their jeans pocket had a gun in it, you would know it. There is no cause to dip inside there and remove the little baggie of drugs. Besides, the police will find all the bad stuff when they search him or her. Methods of searching are coming later.

Use of Force

Use of Force, I think, is where everyone screws up. That is our fault for lousy training. You must start with a policy. Is it hands off, observe and report? That is fine, but as I mentioned, there will be times that you will be negligent if you do not use force. Will you arrest for your own protection only? Such as being battered. Some companies do not allow for this, which could lead to trouble legally if the officer gets his butt kicked and is not allowed to take any action. Or perhaps you have the extreme of these policies with well-armed, well-trained commando-style officers that use force daily. There are so many scenarios and considerations that you need to sit down with your boss, the company lawyer (she must defend you, after all), the local police, and look at your competitors. (You should have done this as part of your risk assessment.)

I have two illustrations for you:

I know of a data center that uses security as a selling point for their product, which is protection of data. They provide a place to store data, operate servers, and make transfers in a secure environment. This is a big deal for companies that hold dear their proprietary information, government secrets, personal identifying information, and the recipe for Coca Cola (author is laughing again).

They provide tours to most people to sell their services and to let the word out that you do not want to mess with them. They start with a background check by having you submit your ID in advance and to sign a non-disclosure agreement. When you arrive, you are checked on the list, the gate is opened, and you are directed by an armed "soldier" where to park. Humvees are strategically parked around the perimeter. When you enter and your ID is confirmed, you are provided an escort and brought into a sally port. This is a mysterious process that makes it feel like you are being scanned or x-rayed or examined in some way. There are more armed soldiers behind the tinted glass and racks of guns are visible behind them. The lighting is darkened, colored highlights, diamond-plate walls and all of that. The tour includes many more "secret" security measures. If you had some important data, you would probably consider using this place as opposed to a suite in an office building downtown.

I call this type of security, "Security Theater." I have two points to make from this story. One is that if you are going to display this level of force and ability, you better be prepared to use it and trained to use it.

The second one is a result of the October 2017 shooting in Las Vegas. If you are not familiar with this shooting in detail, please read the FBI report available online because many of our security measures changed on that day. There is at least one chain of casinos in Las Vegas, that prior to that incident, were considering armed response teams (like SWAT teams) that would be on standby to respond to an active shooter. The initiative was canned due to costs, training, turnover, and the inability to find qualified persons. After October 1, guess what happened. One hotel/casino activated that program, and many others, including dogs, metal detectors, and weapons policies. This example also illustrates the need for training to back that kind of force. The other is that, depending on your risk assessment which considers environment, history, and competition, you may have to step it up a notch if that kind of event is foreseeable.

I defended a casino which had a "hands-off" policy written into their employee handbook. It was one sentence. When a guest provoked a fight and got a whooping, he sued the casino. Security had gotten there right away but basically performed crowd control until the police arrived. Does it sound like the casino was going to lose this case? Well, my omission of fact to you was that the Gaming Commission in this jurisdiction required that a number of police officers be assigned to the casino to keep the peace and respond to such incidents. So, I argued that in that case, a hands-off policy was reasonable as the police were literally seconds away and a security officer would probably make it worse if he got in there and started wrestling before the police took action.

Back to the Use of Force policy. I recommend leaving words like "hands-off" or other such restrictions out of it because there are too many exceptions and it could get you in more trouble. For years—decades, really—the police have described use of Force as an escalation of tools and resources until you land on the right one that works, without being excessive. This is understandable to most cops, but not to most juries. A jury will generally wonder why a taser was used, for example, when two officers were present to gain control of the suspect. Or why the protester was beaten with a baton for spitting on the officer. If that is difficult to explain in court after a police officer receives four months of training, imagine a security officer trying to explain it after four days of training and even less experience using that force. Police officers practice every day, making arrests, breaking up fights, responding to domestic or gun calls, but we may see that kind of incident a couple of times a year—depending on the place.

Rather than trying to explain and teach the “ladder of force,” I find it simpler to train “use that amount of force reasonably necessary to effect the arrest.” Let’s dissect that phrase and see what it means.

Notice the objective is “arrest” instead of “defeating the suspect” or “stopping the attack.” Again, we only can use force to arrest people (look up the exceptions to this please). That removes many of your problems, such as bouncers in nightclubs who think they are Patrick Swayze (look that up if you are younger than me) and forcibly eject rowdy patrons. Weekly, daily, hourly reminders of this policy are not enough. Repeat repeat repeat.

“Amount of Force necessary” does not mention guns or tasers or clubs or pepper spray. The tools you provide are another subject we will cover later. If you had an old woman waving a kitchen knife at you, would you use one of those tools on her? You would be justified with most ladders, but most lawyers would tear you apart and so would the media and your other guests. The amount of force necessary for someone half your size with half speed of your reflexes is probably very little. By the way, I am not going to give you the right answer because the right answer is in the head of the officer and what he/she perceived the threat to be. Not what you thought the next morning after your third cup of coffee.

“Reasonably necessary” means what would a reasonable person do? Not the taser, not the gun, not a broken arm. Perhaps there is no amount of force necessary. What if we just contain her until the police arrive? Or her grandson talks her out of the knife. So many options.

I carried a gun as part of my security job at one time. I responded to a panic alarm at the parking booth at about midnight where a 70-year-old, 30-year employee sat all night collecting money for parking. All he had was the panic alarm. A car pulled in and the driver pulled a knife and robbed the attendant of his money. This was a garage entrance so after he got his money he had to drive into the garage, turn around, and exit. I sauntered out there to check the alarm as the car was leaving the booth and heading down a dead-end ramp. The attendant told me he had been robbed at knife point (a felony) and pointed out the car. I gave chase—meaning I walked down behind the car to see where he was going next. I had drawn my weapon, called for police and backup, and threw my radio in the trash. A clever diversion? No. I had my radio in my right hand and my training was to keep my right hand free for the gun, so I instinctively cleared my hand (author is rolling on the floor laughing again). Anyway, it turned out to be of little consequence. I had my gun out because that is what one does in the movies when chasing a knife-wielding driver of a 67 Pontiac. The car turned around and started toward me at a high rate of speed (another phrase found in chase reports). As he approached, my firearms training (muscle memory) kicked in: I shuffled to my left behind a van, extended my arm, and put that driver right in my sights. It was slow and smooth, and I never felt so confident in my life. Just like in the movies, time slowed. Seriously. I felt like I had all the time in the world, and I considered my options. I had a clean shot, there was no background of any significance, no crossfire by responding police, and his intent was clear as the windshield of a 67 Pontiac. I thought about the consequences of my actions: a shooting that might damage the hotel's reputation, the inquiry I would face, the lawsuit his family would wield against me, and if it would haunt me in my dreams forever. Nahhhh. Then I considered my other option which was to stay behind the van and let him pass me and leave. It is not like he was going to shoot me with the knife and the van option was so clean and simple. So, I kept the gun trained on him from my advantage of cover and watched him leave. I got his license plate, and he was later captured and identified by me in a line-up and, well, it was Nevada so he got ten years for armed robbery.

If I must say, I had a level head which saved my company a lot of time and the firearms program a lot of scrutiny. People do not like guards killing anyone.

My lessons learned: Muscle memory is a real thing. Always carry the radio in your off-hand. Consider your options in advance so you do not have to make a life-or-death decision from behind a van. Even though the amount of force may be reasonably necessary, legal, and within policy, it was still a last resort, not a first one. Retreat may be the better option for everyone. We took the old guy out of the booth and put him inside after that and automated the parking system.

Use of Force (More Stories Later)

Before you start training Use of Force, you need to know what your policy is. Consult the others as mentioned above and call in an expert if you are not completely confident in your policy.

Once you have a policy, train train train. Your objective is Safety. Your second objective is defense—of your policy in court. Imagine each of your security officers in a deposition answering the question: "What is your use of force policy?" Rather than go down the windy road of ladders and escalation and hands and guns and tasers and less-than-lethal weapons, keep it simple. The answer is: "We can only use force that we have to use." Everyone understands that and it is easy to remember and it is the Golden Rule of Security.

Most officers and their managers do not realize that even though they have a "no force" or "hands off" policy, they still represent two rungs of the ladder of escalation. Let's go through them.

Physical Presence—That's right, just being there is a level of force. In fact, it is one we do every day, and in official security language, it is called the "deterrence" component of protection. A professional security officer, outfitted in a proper uniform, with badge and all the accoutrements represents the first level of force. While it does not look like force, picture the officer walking into a room where some kids are about to use a spray paint can on one of the walls. They see the officer and take off. That is a level of force.

Verbal Commands—I think, by far, this is the most common and most under-estimated of the levels of force. Two people are involved in a fight and you yell, "knock it off." Whether that is effective or not, it is a use of force. "No running!" "Get off the grass!" As I mentioned before, most untrained persons would question why you did not even attempt verbal commands before resorting to "violence." The verbal command is so serious, that in most states ignoring the commands of a police officer is against the law. You can take that a step further by saying that refusing to leave the property after being warned to leave, constitutes trespassing.

A case in Nevada that went all the way to the state Supreme Court questioned why, when a security officer was waiting for backup to break up a fight, she did not attempt to stop the violence with verbal commands. Her waiting for backup (as she was trained) was perceived as inaction by the court. After that, we started teaching officers to use verbal commands to stop violence while waiting for backup to arrive.

"Soft" or "empty" hand controls—Here is where this gets confusing to security officers because we try to parallel the police in their policies, but we really do not have the same latitude as they in touching people. Your policy should be: "We only touch people as a means of placing them in handcuffs." If you have a "hands off" policy, then why would you be touching anyone? Of course, there are reasonable exceptions, such as assisting someone who is having difficulty walking, performing CPR or other medical care, and so forth (that comes back to intent, which I mentioned earlier).

Soft hand controls are generally described as those moves that are not intended to cause injury or severe pain. These can include some wrist locks, arm bars, pressure points, and most importantly, application of handcuffs. Legally, we get into trouble at this level because we see security officers pushing people, manipulating their arms and hands, and often without arresting them. Certainly, if you have seen a bouncer in a nightclub ejecting a drunk, you have seen some sort of pushing or "force" used to gain compliance in leaving.

Usually, there are no ramifications because the person being ejected thinks it is part of the process, there are other justifications that will mitigate a use-of-force claim. One is the perception of the officer applying the force. If she can articulate that the person could not stand or walk on his own, or that he was endangering others by bumping into them or swinging his arms, most reasonable people would support her actions. Remember that applying physical force to anyone is "battery" and moving someone—or not letting them move—is a deprivation of liberty—and both are crimes. We do not have the authority that police officers do to use reasonable force while investigating suspicious activity or crimes, so we must treat everyone the way we would expect to be treated—and only use force necessary to effect an arrest.

Intermediate weapons—The police, who have all these tools and abilities, normally separate this level into two or three levels. If you have some or all these tools, you may want to do that as well. The person that teaches you to use them will explain where they belong. This level, as I have combined it, includes batons, Tasers, and pepper spray and all their variations.

Lethal Force—Just because you do not carry guns does not exempt you from understanding this level of force. Deadly force can be applied with a car, or a baseball bat, a chokehold, or a Molotov cocktail. The weapon is less important in this ladder as the way it is used and the intent when using it. Security officers, regardless of the policy on use of force, must understand their limitations when using force.

Company Policies

There are topics that need to be covered in a classroom setting that are unique to your company, your property, and your department. Some of these are presented in a new hire orientation by Human Resources, perhaps. But the specific security policies may not. Some examples of topics to be covered in this section are Uniform Appearance, general conduct, discipline, scheduling, absence policy, parking rules, and on and on. Remember that some of the details will be taught by the FTO (field-training officer), but certain things need to come from the trainer's mouth to be kept consistent.

Report Writing

Another area where security departments lag is documentation of incidents. Some departments choose to train report writing to more seasoned officers for several reasons. First, it is a difficult class for many. Unfortunately, the classic security applicant's command of the English language is weak. Paragraph and sentence structure, grammar, spelling, and storytelling are lost on many of our high school graduates. Second, it may be too much for a recruit to have to learn the geography, the policies, patrol procedures and then compound that with an investigation and report.

Note that I mentioned investigation before. That is right, a report requires a preliminary investigation. That is what a report is. One area where we can compare our organization to a police department is this one. A police officer responds to an incident, such as a burglary report, collects evidence, takes pictures, interviews witnesses, and compiles it into a document. That goes to the detectives, who expound on that investigation and try to fill in the elements they need. We do the same thing, except we are not trying to catch the perpetrator and enforce the laws as much as we are trying to cover the property and provide Risk management with the facts they need to deal with a claim.

Whatever your view on security officer's writing reports, it should be presented in initial training, at least as an overview because they will be exposed to reports and you may find someone that takes to it naturally.

I will go over reports much more in depth in the Investigations Chapter.

Emergency Procedures

> Boy, that escalated quickly.
>
> *Anchorman* Movie

Emergency procedures require hands-on training, but the classroom is a place to explain why we do what we do, the objectives of our plans, and who does what.

Many new hires, if you asked them on day one, what their duties are when a fire alarm goes off, might surprise you with their answer. Putting out the fire, running to safety, or resetting the alarm might be some of the wrong answers you would hear. Same goes with Active Shooter and others. Use the classroom to explain that our first priority is the safety of ourselves, our guests, and our employees. We act as a liaison with first responders, providing our specialized insight of our property, and dealing with guests while they extinguish a fire, apprehend a shooter, or whatever.

When a new officer knows what our objectives are, he will understand the procedures as they are explained and will learn them faster and better.

Guest Service

Security Departments, in general, are not the greatest ambassadors of guest service. It is not organic and depends entirely on management as to whether there is an emphasis placed on it. In my opinion, security should be the best at welcoming and taking care of our guests. We are usually a little better trained than other departments, know the property well, and have the unique advantage of being everywhere all the time. Unfortunately, we tend to focus our training on the specific skills and not on those who pay our bills and create the hospitality environment.

Most hospitality companies have specific service requirements and I recommend following them and exceling at them. This starts with you and trickles down through your managers to your staff. There are two rules I would like to instill in everyone. First, hire attitude and train skills. You can easily train anyone to look for safety hazards and patrol hallways, but you cannot change someone’s personality from grumpy and quiet to friendly and outgoing. Second rule is, consider how difficult it is for an officer with limited life experience to go from enforcer to greeter in a minute. From aggressive to sweet in an instant. Think about your school teachers over the years. Some were sweet and kind and all the kids loved them. Others were strict and mean and did not let you get away with anything. And just a few, maybe a couple, were firm, but fair. Gentle, but serious. Those, I would argue were the most successful. Similarly, security officers may be greeting a family who arrives for vacation, then dealing with the drunk father later at the bar.

I recommend role-playing to hone officer skills. The more latitude you give officers in what they can do and the resources they have, the better they can care for guests.

This section of your training may also include policies that deal with Civil Rights, protected classes, and other discrimination issues. The Americans with Disabilities Act (ADA) is an important one for officers to know, as well as your policies on pets, racial complaints, and even HIPAA (Medical privacy laws).

These are what I would consider the minimum requirements to be included in a new-hire academy. You can add your own unique classes to your academy to make it more rounded and definitive of the style of your department and company.

Director on Trial—A man in a wheelchair is staying at your hotel with his small dog that usually sits on his lap. The man gets a little tipsy at night and starts “dancing” at your bar with the live DJ. The man is unkempt, dirty, stinky, and his dog is barking at all the other patrons who are dancing. Security is called and they tell the man to go back to his hotel room for causing a disturbance. After he refuses a couple times, they evict him from the hotel.

Mr. Director: What is your policy on evicting persons who are protected by the Americans with Disabilities Act? Do you evict all of them or only those who do not meet your physical standards of being able to bathe themselves? How often do you evict those with service animals? How do you decide if it meets your definition of a service animal? What training do your officers undergo to make these decisions? How many other war veterans have you evicted from your hotel?

These polices cannot be decided on the fly and they cannot have so much gray area that it allows the employee to make such a serious decision. Review your policy on service animals, ADA accommodations, Evictions, and even hygiene with your Legal or Risk folks and make the subsequent policies crystal clear to ALL employees.

FIELD TRAINING

I mentioned before that “shadowing” or “walk around the new guy” is no longer acceptable, especially in security. Training is not only vital to a healthy operation, but it will be closely scrutinized by many entities. I always think of training as a representation of me (and each manager should think this way). So skimping on training shows me and others that you are not invested in your staff and do not care about the outcome.

After we talk about quality training here in a minute, we will discuss the important part, which is documentation. Having a detailed recording of the training will defend the program to those who would consider it inadequate. After all, it is just as easy to call your training weak, as it is to call it strong, if there is no record of what is done. Beyond that, a record of just one’s training is also insufficient. You may be asked to show the consistency of your training as well as just one officer.

Director on Trial—A woman passes out in the hotel lobby. Paramedics are summoned and security responds and arrives quickly. It is decided that the woman is intoxicated and not responding to stimuli. Thus, nobody brings the AED (Automatic External Defibrillator). Paramedics arrive on scene a short time later, connect her to their AED and find she is in cardiac arrest. She is whisked out of there and dies at the hospital.

Mr. Director: Why do you have AEDs? Who decides which calls should have an AED? If officers are all trained consistently in their use, and you have AEDs standing by to save lives, why wouldn’t you have one brought to every medical scene? Do you wait for paramedics on choking incidents? Drownings? Falls? Or just when your guests have heart attacks?

The death may or may not have been prevented by using the hotel’s AED, but we will never know. Expectations of your training are: (1) Competence and

(2) Confidence. Competence is proved by consistent, documented training, but confidence is judged by family and bystanders that either see you doing everything you can or waiting around for more competent personnel. This hotel lost this case because there is nothing a director can say to defend the inability of his staff to try everything they reasonably can to save lives.

Can you imagine hiring a really effective trainer to come in and teach your entire staff how to do something—such as guest service, handcuffing, or investigations. Then a year later, you are having to prove that the training occurred and all you have is an invoice. A complete waste of time.

Our FTO program, therefore, will be documentation-centric and not just following each other around. Before we start field training, we need some FTOs. FTOs are selected based on their experience, aptitude, and attitude. Your new recruits are going to spend a lot of time with FTOs, so their attitude and ability to teach is especially important. Teaching skills can be taught through an instructor development or similar program. In an ID program, FTOs learn how to make presentations, identify learning styles, and use the "explain, demonstrate, observe" method of teaching tasks. They also learn how to give constructive feedback and correct unacceptable behavior.

Rather than just selecting the most knowledgeable officer to be an FTO, make sure he or she is going to be able to "sell" the job to the new employee. The last thing you want is someone who will teach bad habits or badmouth the company for eight hours. You may want to have tryouts and some sort of testing process to make sure you get motivated employees to take this position.

Being an FTO is a huge morale lifter and a goal to which many "plain old" officers can aspire. Almost anyone can be trained to be an FTO and once they have that instructor certification, their pride will increase, their quality of work will improve, and they will raise the collective bar for their peers.

Task List

Once you have your trainers trained to train trainees, you need an organized training process. To structure the training, it is best to start with a task list. The task list is made up of every job that a security officer does, no matter how insignificant. Everything is listed from common patrol procedures to fire extinguisher inspections to guest interactions to report writing. The task list may be several pages long. If you get writer's block on this, try using your daily logs as reminders or have your FTOs make notes of their activities for a week or so. Once the list is compiled, create a form where the FTO and the trainee initial each task as they show proficiency.

The task list may determine the length of your field training. In a large hotel, two weeks is probably adequate. If you are not sure, look at other comparable hotels and make sure your training is at least equal to theirs. If that is not helpful, you may have to run a few trainees through your new field-training program and see how long it takes them to feel comfortable and confident on their own. The daily reports will help you make that determination.

Evaluations

Observation reports should also be created for use by the FTO. This one-page evaluation form lists several categories in which to observe the trainee's progress each day or whatever interval you choose. These categories include guest service, knowledge of property, officer safety, knowledge of procedures, etc. Next to each category, place a 1 to 5 or 1 to 10 scale in which the FTO circles the number corresponding with the trainee's performance. Each substandard and each above-standard rating is explained with a comment. The FTO reviews the report with the trainee at the end of each day to let him know what he did well and where he needs to improve. Trainees are kept in training until they meet standards in every category.

The supervisor should also do a periodic evaluation. This gives an extra set of eyes to the evaluation report and ensures that training is being administered fairly and consistently. The supervisor reviews his observations with the trainee just as the FTO did.

These three forms of documentation—the task list, the daily observation report, and the weekly observation report—show in a detailed fashion exactly what was trained and how it was trained. If all aspects of training are covered in your list, it will be difficult for anyone to accuse your company of having inadequate training. On the other hand, if you have an employee with consistently low evaluation scores and you pass him on to regular duties, you may be considered negligent. There are also some training classes or modules that will be too intensive for a task list. These include CPR, weapons, defensive tactics, bomb awareness, etc.

IN-SERVICE TRAINING

Some training programs end after the initial days and hours, never to be spoken of again. Remember that we must repeat, repeat, repeat, to get things into muscle memory. The Officer Development Program (discussed elsewhere in this book) is a process that ensures ongoing training and kind of runs itself if you have someone to coordinate it. Whatever your method, there are three reasons to keep training current after the new-hire training is complete. First, there are several required programs to be taught that were not covered in the initial training: CPR and defensive tactics, for example. These classes are also difficult to pile onto a new hire who is absorbing so much in a short period. They are not needed during the field training anyway. Second, procedures change and are added constantly, so we need to keep everyone updated. These include emergency procedures and various specific incident responses. Third, in-service training keeps officers fresh on various procedures that we do not want them to forget but may not happen very often. Defibrillators may not be used very often, but, on a regular basis, we need to make sure officers can show proficiency.

There are several methods of providing in-service training to your staff, and I recommend you use all of them. Note that this is training above and beyond the initial training done after hiring.

Classroom—Officers need to be pulled away from their duties on occasion for a class. Lecture or workshop classes are good for teaching CPR, first aid, defensive tactics, and other intensive multi hour programs. Make sure officers are paid for these classes, that the instructors are qualified, and that attendance is documented.

Briefing/pullout—If you are fortunate enough to have a pre-shift briefing for your officers, there are many topics that can be covered in a few minutes. Handling agitated persons, resolving guest complaints, or handcuffing refreshers are good topics for these short presentations. During shift, pullout training can be done with minimal disruption. This type of training can be discussion/tabletops or actual exercises. Fire drills, active shooter scenarios, CPR practice, and many other topics can be covered daily. Make sure each officer gets a chance to participate and that it is always documented.

Tabletop—A tabletop exercise is the best way to train officers without disrupting business. Officers gather around a table in a workshop format and run through a scenario. Upon being given a scenario, each officer relates what actions he or she would take. More information is provided and then officers continue updating their actions until the situation is resolved. This is a great way to train, but also to test procedures to see if they work and if anything was forgotten. Emergency procedures can be developed or tested using this method and then modified as necessary—all while providing training to those who participate.

Debriefings are another type of tabletop exercise. After a significant event at your property or even one that you hear about in the news, officers discuss their actions or the actions of those involved and observe lessons learned. They decide what could have been done better, what worked well, and what did not. Debriefings are an emotional release for the ones who experienced a traumatic event and a learning moment for everyone.

Drills—A drill focuses on one component of a procedure, such as an evacuation drill or a response drill. These take a bit of planning and coordination. You can include other departments and select a time where you do not disrupt business or guests who are relaxing. However, do not be afraid to let guests see you practicing. Get a big sign that says, “We are practicing to keep you safe,” or something like that and let people watch you do CPR on a mannequin or handcuff a fellow employee. Remember documentation.

Exercises—An exercise is training that involves all of the components of a plan. For example, an active shooter exercise may include the response, setting up a perimeter, dealing with phone calls and upset guests, and triage of injured persons. This training can be as large and as complicated as you want. Full-scale exercises are discussed more later.

DEFENSIVE TACTICS

We talked earlier about Use of Force and the classroom portion of arrest training. I call this physical portion “Defensive Tactics” for a couple reasons. It needs to be engrained in everyone’s soul that any force we use is defensive only—with no exceptions. Any incident that becomes physical with security officers is “defensive.” We should not be taking any action with anyone where we are “offensive.” Our physical actions are to protect ourselves or someone else from harm. Because we do not arrest people for warrants or something they did outside our presence, even an arrest is made in our own defense.

If you are expecting to learn defensive tactics from a book, or for me to present it here, you are sadly mistaken. These maneuvers are so critical that it requires a qualified instructor to show you and your team physically and personally. Please do not attempt to get these skills from a book, a video, or any other medium.

A common way to introduce these tactics to your team is to get a qualified instructor and have him/her train your trainers to pass the maneuvers to everyone. There are no security industry standards of training for physical control techniques, so you need to be careful of your source for your training. There are some private firms that tailor classes to fit security officers. Make sure that they understand your use of force policy, so they are training the right moves and levels of force. Same goes with police officers or ex-police officers, academy trainers, and private firms that train police. Police have different laws, different objectives and abilities, longer training, and different immunity than private security officers, so again make sure your instructor understands that before developing a training program.

Defensive tactics include everything from officer presence to deadly force. Because consistency is one of the keys to training, we must teach everyone the same tactics in the same manner every time. Use of a qualified instructor is the only way to do this physical training. Many police and military training programs employ a form of martial arts for their defensive tactics training. This does not mean you should go over to your local dojo and hire sensei Bob. It does mean that you find an instructor who not only knows the moves, but also the legalities, liabilities, and medical dangers.

Sudden in-custody death syndrome is a term given to deaths of uncertain reason following an arrest. The cause is often (but not always) drug-related and can occur during, immediately following, or days after a violent struggle. Researchers are still investigating ways to prevent it medically, but in the meantime, there are precautions we can take and responsibilities we have to those in our custody.

Besides the consistent, strict adherence to training and procedures, arresting officers should have a protocol for tending to persons in handcuffs. First, ensure that the fight is over. Once someone is restrained, it is no longer necessary to apply pain or restrictive holds unless those moves are defensive. Second, prisoners should be monitored closely for abnormal breathing and other signs of stress, shock, heart failure, or injury. Third, any signs of anything unusual should be reacted to immediately. This includes first aid and calling emergency medical services. It is better to be safe than sorry.

I cannot tell you how many times I have seen security directors provide handcuffs to their officers on their first day with no training. You might as well give them the keys to the company safe. I cannot think of a more costly mistake than to give an untrained officer handcuffs—except maybe giving him or her a firearm. Even an untrained officer with a gun would probably not be as bad because most people realize the seriousness of pulling a firearm. Instead of speculating what is worse and what are the risks, let us just agree not to provide those things without proper training.

Handcuffs are a necessary tool for security, but dangerous legal exposure comes from depriving freedom especially by force. This liability is discussed in more detail in the next section.

A chokehold is a common name for either of two holds called the Arm Bar Control and the Carotid Control. The Arm Bar Control is one arm around the front of the neck, using the other hand to pull back on the arm bar. The effect is to cut off the windpipe and decrease oxygen to the heart and oxygenated blood to the brain. The Carotid Control places one arm around the neck (from behind) with the elbow at the front. One arm pushes against the other arm, creating a vice. This cuts off blood flow in the carotid artery and the jugular vein, decreasing blood to the brain.

Between 1975 and 1982, the Los Angeles Police Department included a chokehold as part of their use of force policy. Sixteen people died as a direct result of the chokehold and it was finally restricted to use only in life-threatening situations. Physicians deduced that the desired effect of compliance and loss of consciousness were often preceded by the undesired "fight or flight reflex" where the prisoner actually resisted more because of the fear of death. The desire to escape—which is a conscious decision—is overcome by the will to survive—which is instinct. During this resistance, the suspect uses his instinctive final breaths and energy trying to stay alive rather than complying with rational commands.

Anytime you put your hands on someone, it had better be to make a lawful arrest. Except for catching someone from falling or helping in a medical situation, any time you touch someone you are stepping into a legal situation. Placing someone in a wristlock, pushing a drunken patron out the door, or placing handcuffs on a possible shoplifter all constitute false imprisonment and are subject to legal consequences, unless they are pursuant to a lawful arrest. The scenes you see in the movies where the two bouncers throw the bad guy out the door are for Hollywood and have no place in our business.

Remember that police officers can use hard hand controls to modify behavior. They have legal authority to lay hands upon people where we do not.

Officers who are equipped with weapons of any kind should have these incorporated into their DT training.

DOCUMENTATION

I am not sure I mentioned documentation enough times in this chapter. If training is not documented, it did not happen. All that work is a waste of time if it cannot be proved to have happened. Keep training files for each of your officers separate from their personnel files. Track every piece of training they receive. These records will be subpoenaed when you are sued for inadequate training and that is great. Most lawsuits due to training inadequacy are lost by hotels that did not have documented training. You want the most well-trained, well-equipped security officers in the world and with some work you will meet that goal.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

4

Staffing

> *The best way to appreciate your job is to imagine yourself without one.*
>
> —*Oscar Wilde*

You may know I come from a background of managing proprietary security forces and I tend to lean that way with my anecdotes. However, I have worked with many hotels that either use contract security companies or no security staff at all. In fact, I am not lost on the fact that the portion of the world's 700,000+ hotels having proprietary security is in the minority. I will try to address each of these three categories here and I urge you to read about each one, as there are some nuggets for you in all of them.

People are the core of the hospitality business. Security officers sometimes think they are exempt from the hospitality part, which makes it harder to recruit and hire good ones. Of the many traits necessary for a security officer to have, finding all of them in one person is a challenge. As one of my officers used to say, you need a person who can walk a little old lady to the restroom one minute and confront a drunk refusing to leave, the next. In other words, a combination of intelligence, friendliness, and physical ability is what our objective is. We can compromise on those abilities a little without compromising our integrity as you will read shortly.

GUARDS OR OFFICERS?

Let's get one piece of terminology out of the way first. You may have noticed that I refer to security personnel as "officers"—or "professionals" in the case of management. Many people in our industry and in society refer to uniformed security as "guards." (This is even more common on the east coast of the US for some reason.) I find the word "guard" to be inaccurate and condescending, like calling a "chef" a "cook" or a "corrections officer" a "prison guard." Setting aside the emotion, look at the way the word is used in other contexts. A guard is used to describe the piece of metal that keeps the chain on your bike. In my mind, a guard is someone that has a binary function, such as letting you in a door—or not. A guard sits in a guard shack. He does not perform CPR, take incident reports, listen

DOI: 10.4324/9781003037644-4

to guest complaints, refer someone to the best steak dinner or handle triage for an active shooter. Security Officers do that.

I acknowledge that we need guards and that we have guards stationed at doors and gates here and there. But in the hospitality world we use security for everything except guarding doors. Officers' training and their experience cause them to make complex decisions and to manage many tasks simultaneously. If this is just semantics to you, please indulge me and call your officers by the name that best describes their importance. If it is also important to you, help me correct those that are uneducated on guards vs. officers.

HIRING

We begin with proprietary security. Contract security is coming later.

Hiring, training, and good management make up the three legs of the staffing stool, all being equally important. Unfortunately, each component is time-consuming and requires skill and experience. Delegating these tasks to the wrong people—or the wrong department—is a mistake.

Recruitment

When I first wrote about hiring a couple decades ago, it was like fish in a barrel. The problem was selecting the right one out of a sea of applicants. Several variables have changed that to the inverse. Unemployment is at all-time lows. (Job market is small.) High-tech jobs and tech-related jobs have moved into most metropolitan areas and gobbled up the same people we would recruit for our hospitality venue. In the area where I worked last, several huge companies came to town and hammered our market, hiring about 5% of the total population in a one-year period. They paid much better, had better benefits, great shift times, and apparently low requirements. That left us with nothing. Applications dried up.

The knee jerk answer was to raise starting wages to compete with the new kids. Well, that was about a half million-dollar increase (We had a large complex) and a couple of hotels went for it. It helped them a little, but not a half million dollars' worth. I tend to take a more analytical approach to problems like this, so rather than throw money at it—which I did not have anyway—I tried some less costly solutions. If you are also having recruiting problems, try some of my ideas below.

First, let's examine the traditional method. By traditional, I mean you put up a job posting and wait for someone to come in and get excited about it. Then you have a Human Resources Clerk—affectionately called a "recruiter." That person "screens" them and passes on the winners to you for a second interview. Consider each of these steps and how dysfunctional they are.

Job Posting

This is a passive method that used to work when the scales were tipped in our favor. Hundred people daily, walking into the employment center, and you could pick up a dozen of them with just the posting. The posting assumes that your visitors—they are not applicants yet—are really interested in getting a job, as opposed to completing a regulatory requirement to get government benefits. Then it assumes they know they want to work security. Did you know you wanted to work security when you entered the job market? Many of my best officers came in looking for a job in another department because they did not think they qualified: They were female or small in stature or ignorant of the job or their spouse will not allow it, etc. There are those who have no skills, so they think they only qualify for security. Finally, your job posting is competing with every other department and it does not stand out. Same benefits, maybe lower pay, high school diploma, driver's license, clean background, drug test, blah blah blah. Same as cook and housekeeper.

You may notice I do not care for the job posting in HR. If you are going to have one, make it stand out! What do you have to offer? How about free training? How about no experience required? How about a cool uniform? What else you got? Do some marketing.

The Screener

How many good people are you losing to this stage of the process? I have worked with good screeners and with bad ones. The worst one I had was a racist woman who was discreetly directing the Hispanics to housekeeping, blacks to the kitchen, and never a woman to Security. This is an extreme example, but true, and I doubt you have anyone this bad, but it is an illustration of the power that one person has over your department. I would get with the HR director and tell them you will do your own screening. We appreciate if HR will just make sure they are of age and legally allowed to work, but we will vet the rest ourselves. Take it a step further and bribe them. Buy them some ice cream. (That was my partner's idea.) It worked wonders. Now, if you have great screeners now, forget what I said. Do what works for you, but do not let this part of the process be a hurdle.

Qualifications

Back to the qualifications. Many security departments seek prior security or law enforcement experience. Ask yourself if these are your best candidates. We usually like this experience because they may need less training or acclimation to our type of organization. Usually there is a tradeoff of skills for attitude. I would argue that a corrections officer, an army sergeant, or even a homicide detective is not necessarily suited for the hospitality environment. They may be better at handcuffing or dealing with violent suspects, but do not lend themselves to the customer service environment in a private business. I have found that it is easier to train a former restaurant host how to handcuff and deal with hostile persons than it is to teach a drill sergeant how to provide great service to a family in the hotel. Now, this is not to say that I discourage hiring anyone from the military or law enforcement because many of our best security professionals are from these fields. All I ask is that you not use this experience as your primary qualifier or even a prerequisite. You can train skills, but not attitude.

You may have some requirements that may be unnecessary and eliminating some good employees. "Valid Driver's License," for example, may be a little outdated. Do your officers really do that much driving? Do all of them have to drive? Do you have motorized patrol? Do you have to? Something to consider because many people, especially in the lower end of the job market, do not drive.

If you have a good team in place already and you want to add more just like them, have your team help with recruitment. A good portion of their friends and colleagues probably shares their attitude, work ethic, and experience. These referrals take some of the unknown out of hiring. It may be worth the cost to offer a finder's fee to your employees for these referrals. Another good source of recruits is employees from other departments. If you see an employee who possesses a great attitude and customer service skills, see if he wants to transfer. Most of the time, they have already considered it, but never imagined you would hire someone without security experience. They do have hospitality experience and you have already had a chance to watch them in action. This employee is not an unknown and you can easily train him or her technical stuff, but you cannot train attitude.

Starting Wage

Personally, I do not believe in giving "across-the-board" increases, which is what you have to do to hire someone at a higher rate. Though we have done it before to "catch up." (Just using round numbers: If you have been paying $10.00 and you want to hire the new guy at $12, then he will be making more than guys who have been there a year. Although you do not have to raise everyone, you will struggle with morale issues.) I created a scale that we called the "Officer Development Program" which is explained later. It gives raises based on skill level and experience.

As I mentioned before, it is expensive to raise wages. The math is straightforward—$1.00 per hour is about $2,000 per year per employee. So, multiply 2,000 by number of employees. This does not include cost of benefits. The higher, the better; so if you can get higher wages, go for it. Beyond that, here are some other things you can do to increase interest in your job posting.

Loosen Up

I found that in the job market I was in, we needed to get real creative if we wanted hireable applicants. Here are a couple of things we tried. Consider creating a job position in your department that is just "below" security officer. Drop the age to 18 years old; High school not required. Put them in a different uniform and call them Guest Service Officers (GSOs). (I thought this was my idea until I realized the police have been using "civilians" for administrative tasks for years.) Use the GSO for high visibility, giving directions, and doing "guard work." Pay the position a dollar less than Security and see what happens. I think you will find that many people who do not meet your qualifications for security officer will be very good at this job. Some people do not care about the wage, but they do not want to confront aggressive people. They want the great insurance benefits and to meet people. Perfect. I had one lady that wanted to work security so bad. (She worked in a restaurant and hated her managers.) Her language skills were not good and when we tried to train her on defensive tactics, she just was not very adept. We tried her as a GSO and, wow, did she shine. She became an ambassador for the hotel, welcoming guests, learning their names, greeting, and conversing with everyone she met. She was a superstar that I would have cloned if I could. If I had not been flexible on qualifications, she would still be clearing tables in the restaurant.

Another idea is hiring foreign students on work visas. Many hotels do this already for guest room attendants. There are agents that arrange all the documents and travel and bring you nice fresh faces for a finite period. These may not qualify for a hotel security officer, but they are generally intelligent, speak English, and happy to work for our pay and conditions. Try them in that "GSO" position or for your busy season or special events. One secret about these workers: They want to work hard for the brief time they are in country. You may find that your competitor has already contracted with the agent and your hotel can be their second job. This requires no additional visa or paperwork.

Security on trial. How will you answer these questions?

1. Why do you train foreign workers differently than you train security officers?
2. If Mr. X is not exactly a security officer, why was he sent to back-up a security officer?
3. This post has always been staffed by a trained security officer, why is it OK to put a temporary foreign worker there with lesser training?

Keep the roles separate and distinct. Having more than one job description in your department can get complicated and it requires attentive management.

Application Process

This is another frustrating part of the process for me: The hand-written-come-down-and-fill-out-this-paper-application process. Hopefully, you are not using paper applications. Anyone under age 40 or so, uses a phone for everything and definitely not a pen. Plus, it is not in line with the job so why do it? I bet most 19-year-olds cannot hand-write anyway. Urge your company to step up and go online. And if your company is online, please make sure your application process is one of which you can be proud.

Remember that the HR department is hiring for every department and they are probably focused on the hard-to-hire Guest Room Attendants or Stewards. A generalized application that applies to all positions in a hotel is almost worthless for security. If you can change it and customize it, that would be great. Otherwise, use it to vet the minimum qualifications, background, etc.

Companies that have embraced the online hiring process do everything online. If you can get to this point, you will attract more millennials who are the bulk of your labor market. There are some companies that get a little carried away with assessing character, giving psych tests, and laying out an intimidating gauntlet of personal questions that are better suited to executives, in my opinion. You are hiring for a low to mid entry-level position and you cannot afford to eliminate people just because they are shy or slow with English. I have seen online applications that take hours to complete. That is just not appropriate for entry-level. Someone willing to settle for a low-paying hotel job is not going to spend hours and hours applying for several jobs.

Applications will not go away, for legal reasons, so whether electronic or paper, someone in your organization needs to have some training on reading applications. Besides the obvious legal limitations, there are several nuances in every application that can be gleaned if you know what you are doing. Hopefully you have an application that has some writing or fill-in answers. Check boxes tell you nothing. We are estimating an applicant's integrity when we read an application. Experience and education are irrelevant, except where they had issues or conflict. Here is how I review an application, step by step.

- Use a red pen and go down the line looking for things that jump out. It is much easier to do this if it is a hard copy. And even though I dissed the hand-written application, it is easier to get a feel for things from handwriting. Oh well.

- As you mark-up the app, do not think about disqualifying someone based on their answers, but think about asking them about their answer.
- Look at the handwriting. Sloppy and rushed? Why is that? If typed, short one-word answers? Why is that? Make your marks.
- Do not make marks that appear to discriminate. The address, for example does not concern you. Neither does the year of their graduation.
- Scroll down to the good stuff: education, work experience, and criminal background.
- Red flags on experience are gaps—time spent out of work. Another one is "Why did you leave?" Just circle the answer. It does not matter what it is, because most will lie or deceive on negative answers.
- How do they describe the previous jobs? Again, just circle it because you are going to ask them.
- Education is a similar marking process. Look for gaps; field of study; did they finish?
- Then the criminal question. If this is a yes, it is likely an incomplete answer. Circle that for later.

In my opinion, the application should not be used to disqualify someone (unless they confessed to a murder or something). Some people do not interview well; some do not test well; and some do not fill out applications well. Have a talk with them. Only your time is lost. Use the application to provide talking points for the interview.

Interview

Before the interview, we can already start to evaluate our prospective employee. Have them escorted to your office by a trusted employee—a recruiter or manager or whomever. Make that person your agent who tells you how genuine their attitude was on the walk to your office. Remember that a candidate is on stage and giving his or her best performance during the interview. Attitude and answers are not always genuine, so any intelligence you can derive beforehand is valuable. In fact, in my personal experience, I have found that some candidates treat the HR and support folks like crap and then are all smiles when they get to the interview. This is a better indicator of future attitude with guests and employees. If your HR people tell you that an applicant was rude to them, cut your losses.

As I alluded to before, we have lowered our bar a bit on interviews in the past ten years. Business attire is something you will rarely see. Many times, someone job hunting is broke, and the security field does not require a suit so why would they have one? I prefer a shirt tucked in, but frankly, who does that anymore? Set your expectations for appearance according to social norms and not on your own requirements. Hygiene is different. If someone stinks, do what you feel is right, but in my experience, you cannot fix stinky.

You may learn much more from this pre-interview ice-breaking session than you will from hearing their prepared answers in the interview. How did they find their way? Did they introduce themselves to other people in the office? Did they make eye contact or look at the floor? There is so much information here.

One more thing before we start talking. If your security job involves report writing, have them write a paragraph for you. If your reports are on the computer, or an app, have them navigate that. Look at penmanship, spelling, grammar, and sentence and paragraph structure. These are things you are not prepared to teach and will not have time to do so. If someone cannot form and write a paragraph, maybe you can recommend them for another position in the company that requires less writing. Writing is too important in our department.

> Please open Word and write about 25 words on why you want to be a security officer, or how you traveled here today, or about your last vacation.

Look for computer skills. You don't have time to teach officers how to use a mouse and keyboard. Unfortunately, some of our older applicants still have trouble with mouses (mice? Mieces? Old joke. Sorry) and browsers. If you can deal with that, go for it.

Standard Questions

You should prepare your interview questions in advance. Some will be standard, but others may be unique questions that probe the application.

The objective of the interview is to have a conversation. If you were interviewing for the position of brain surgeon or computer coder, your questions would be much different. All we want is to get to know the personality of our applicant. The answers, in fact, may not be as important as the way they are presented. If your applicant is taking this process seriously, then they will be scared to death. Think about your first interview. That anxiety is not conducive to complete and honest answers or a conversational experience. Here are some ways to get into that conversation and ease off the fright. (By the way, plenty of books and classes on this. My remarks are just one method.)

Start with an ice breaker. Ask a question that gets them talking about something fun. If they have a sports team logo on their clothing, ask them about their team. Did you see the game last night? Or same with TV shows or movies. Military tattoos, whatever you can find as an opening. The idea is to get them talking. It is not a test, but an observation of how they interact with strangers. If you are getting short, yes or no answers, it is because they are nervous. Everyone has it in them so do not give up. As a last resort, tell them they are not getting this job unless they can interact with guests, so they need to open up here.

The Questions

You should have some standard questions that you know are safe. Make sure you have checked with your legal folks, so you do not get in to trouble. For example, you cannot ask about medical conditions ("When are you due?" or "My daughter has that same rash. Is that psoriasis?") Stay away from religion, race, gender, and all the protected classes. If you focus on the job or work and education history, you will be fine. Again, I worry little about the question and instead focus on the answer. Getting someone to brag a little is a great way to start a conversation. (Tell me what you did to earn the employee of the month award at your last job?) Other good questions are: Why do you want to work here, or What do you know about the job here? There is no wrong answer, but there might be too short of an answer. If someone says "the pay," then back to the conversation.

Now go back to the application and your red marks. No need to hide it, it is their application. "I made some marks here so I would remember to ask you some questions. I guess I am nervous also." Simply repeat aloud what they wrote and then "Tell me more about that." Non-judgmental and open-ended. If they put personality conflict with boss, then you are looking for some honesty and not a canned answer. I would love to hear an honest answer, like "He was a jerk who spoke down to people, especially women, so I quit." That is a better answer than, "his personality and mine were not compatible."

Think about the primary trait you are looking for in a new hire. For me, it is friendliness or positive attitude—plain and simple. Yours might be professionalism or proper etiquette, or multi-tasking, writing ability. Whatever it is, see if their answers indicate their compatibility with your department. If they rattle off their accomplishments without a smile, and you are looking for friendliness, you better go back to square one and see if they can do it.

I mentioned before I would rather hire a restaurant hostess and teach her everything she does not know, than hire a 20-year corrections officer who has a bad attitude. A hostess must smile and must be friendly and make conversation in a short time span. A corrections officer can be successful in that job without ever being friendly to anyone. I am not picking on Corrections; it is just an extreme example.

Second Interview

A second interview is a good idea if you can do it. Use one of your supervisors, investigators, or even someone from another department. Use a different format for this interview. Make it more casual, less of a questioning, and more of a discussion. If done right, this will put the candidate at a comfortable level to speak freely. "You survived the interview with the big boss, let's have a Coke and talk. How do you like our department so far? What would you change? What position would you aspire to?" This type of questioning puts you on the same side and extracts attitude and feelings the formal interview will not bring out. If you do not like the candidate from the first interview, do not bother with the second interview.

Group Interview

I really like the group method of hiring, but for me it was exhausting. You need someone, preferably an HR person to dedicate their life to the process and coordinate it because it takes a lot of planning and work. In a nutshell, the idea is to get several applicants in a room and get them to do some team-building, ice-breaking, and problem-solving. It separates the outgoing, positive people from the negatives. In fact, I have seen some people walk out (for the better) because they did not expect to have to go from introvert to extrovert on command. I am not an expert, but if it interests you, check with HR and see if they have an appetite. Unfortunately, if the job market is down, you are not being so selective.

Background

Several years ago, the FBI decided that the integrity of their agents was of the utmost importance. They continue to this day to spend tens of thousands of dollars to check the background of each employee. Their unwritten slogan regarding recruitment is: "Don't hire a problem." While every group of people will have a few bad apples—and they have, this policy seems to have worked for the FBI. They maintain an image to this day of clean, responsible, honest agents.

Does it make good business sense to spend an amount equal to an employee's annual salary on their background? Probably not for a security officer. But in this age of having information at our fingertips, it is negligent of us not to make some simple inquiries. Criminal history is a given, but what about job stability, violent history, drug use, and personal character?

If you do a background check (if you do not, then start today), this is the time to do it. Some of the nicest guys you will ever meet in an interview can turn out to be bank robbers, physical abusers, embezzlers, or dysfunctional alcoholics.

We have all seen guard companies that do a criminal check and a drug test and let the insurance cover the rest. That just does not work in the hospitality industry. We cannot afford to expose our guests and their property to bad character. The loss is overwhelmed by the damage to reputation. Many guests who suffer a loss at a hotel will go online (we used to say they will tell ten friends) and write a review that says something like, "The housekeepers at that hotel will steal you blind." You and I know that hotel losses are often an error made by the guest, but the online review rarely gets rescinded. Damage done.

Back to background checks. Look at the last five employees you fired for stealing. On how many of those did you file criminal charges? I am going to guess, less than half. How many of those were convicted? I will guess again, less than half of those. How many of your applicants may have stolen from their last five jobs? Answer: You have no idea because they are rarely criminally charged. So the criminal background check is only going to catch those who were arrested, charged, and convicted. If you do not check elsewhere, your background check will miss it and thus will be a waste of time and money. There is also something called negligent hiring that we will discuss shortly.

We have to look at the business picture here. A common business reaction to an employee stealing is fire the employee and reimburse the guest or try to recover the loss. This is a business decision that makes financial sense but what does this do to the reputation of the hotel? That guest might admire you for making it right, but deep down he or she is wondering what kind of people you hire and how many are bad that you do not catch. The background for an employee just became important to every other employee on your property and to the reputation of your hotel. Some background checkers will do job history and references, and some will not. If yours does not, you should do this yourself.

Everyone is afraid to check prior employers because nobody wants to give out job information for fear of being sued. There are two things to do to deal with this. One is to check them anyway. Even if the former employer just gives dates of employment, it is a big verifier. Someone who was trying to hide a job where they were fired, or a period where they were in jail, would fudge on their employment dates. A simple check of prior employers would create a nice timeline. Second thing to do with prior employers is call them personally. Do not just call HR; call their former boss. During the interview, you may have asked the candidate: "What would your former boss say if I asked him about you?" You should actually ask the former boss if he or she would hire the person again. This does not violate any policies and it is off the record. This will take away all doubt—or add to it. Never disclose to the candidate what you found in the background check, unless it is required by law.

I think many employers are also afraid to call references because they fear the candidate has primed them. This may be true, but you can still learn a great deal from a couple of phone calls. First, do not ask them the obvious questions. Ask them about a previous job on the application or about a gap between jobs. If they have known the applicant as long as they claim, they will know what he was doing for those four months between jobs. If they say he was in school and the candidate says he was overseas with the Peace Corps, you have a problem.

Many privacy and credit reporting laws, most of them federal, put severe restrictions on what you can find out in a background check. Be sure you use a licensed company or that you are following these regulations and using proper waiver of privacy forms.

Drug Testing

Drug testing used to be a simple, zero tolerance proposition. I highly recommended it and I was a believer. Times, they are a changin'. State marijuana laws really fouled drug testing. The dilemma now is, if marijuana is legal, and it stays detectable in your blood for three weeks, how can you fault someone for testing positive? Even a post-accident drug test has the same issue. There have been some other societal changes in just the past ten years. The abuse of prescription drugs cannot be a reason for disqualification. For one, the user can produce a legal justification for taking the drug (opiates mostly), and two, there is a limit on inquiries you can make to someone who tests positive because of privacy laws. In fact, at one point I wanted to test my armed officers for drugs, thinking that was the responsible thing to do. My company employment lawyer said no. The reason she gave was that so many police officers are on prescription meds for all sorts of things and therefore would never pass such a test. So if police don't get tested why should security officers? My naiveté just astounds me sometimes. But I have other ways of testing my officers' integrity and I will share with you in Chapter 8.

If your company is still doing drug tests, you need to make sure your response to that test is legal and prudent. Are you violating HIPPA (Healthcare Information Privacy and Portability Act)? Are you even violating ADA (Americans with Disabilities Act)? If marijuana is legal in your state, are you going to disqualify someone who smokes a joint on Saturday nights? What about medical marijuana?

If your company stopped doing pre-employment drug tests, then of course you need to be vigilant with all your employees and you need to know the company policy on "for cause" drug tests and ask the same questions about marijuana and prescriptions. If you are not even doing cause testing, we will address that in Chapter 8. I would argue that alcohol is a bigger problem and we do not even test for that.

Before Hiring

One final thing before making the offer, or even if you have already made the job offer. If you find out they lied on the application or during any part of the interview process, fire them immediately. (The cover-up is always more serious than the lie.) I have a strong opinion on liars and I always made it clear with my staff. If you screw up and you let me know about it, I will do anything I can to help you fix it. But if you lie about it, I will not even ask any questions because you just proved you cannot be trusted. In my experience, nobody lies just once and if the person lied during this process, it was to keep you from uncovering something that would disqualify or embarrass him or her. It also means that anytime they do something wrong, they will lie rather than come to me so I have no use for them. Integrity is the most important non-trainable skill your officers will have.

Security on Trial: Please affirm your oath and answer the following:

1. Did you know security officer X had three arrests for domestic battery before you hired him?
2. One of your current officers testified that you do not hire black females. Can you explain that?
3. Your officer that crashed the security truck into my client's car tested positive for marijuana. Do you allow your officers to drive under the influence?

There may be no good answers to those questions, and if there are, you can be sure they will be followed up by a harder one. Keep your ducks in a row on every applicant whether you hire them or not. I know a director that kept a spreadsheet of interviews and why he did not hire persons. A great memory jogger should the subject come up. As long as you are legal, and you should be, go transparent.

Orientation

You need to have two types of orientation—maybe three.

First is the company orientation. Hopefully you do not have to personally do this. It should be done by HR. This is where an employee learns about benefits, company history, the attendance policy, and so forth. No matter who does it, it will be the most boring presentation that was ever conceived. Sorry, friends in HR, but it is difficult to make this anything but naptime. Honestly, I have seen some motivated people try to make this interesting with drawings for prizes, treasure hunts, and trivia games. Whatever you can do, but we must get this information out and, more importantly, retained. Do not be the manager that sends your employees to the slaughter. If your company orientation is bad, help get it fixed. Speaking of which: If you have not attended one, or better yet, spoken at one, put yourself out there. Employees like to see a new face; HR likes to break the monotony; and you need to see what goes on there.

Second Orientation is for the department. Security, especially, needs to be exposed to much more information about the property than a food server or guest room attendant. Your company orientation should consist of your department's internal documentation, uniform fitting, how to wear the uniform, how to wear the uniform, how to wear the uni—oh did I say that already? My gosh, this is a peeve of mine and it should be yours as well. Just wait until I get you to that section—coming up. Where was I? Yes, this orientation may be a bit boring as well, but it has a lot of interaction with the recruit, and it gives them a chance to learn the department culture. This orientation is the unwritten second seed (interview was the first) where we get to show off and instill some department loyalty and arrogance. Yes I said it. We are the most arrogant department and we deserve the title—Pride Building, Team Building. In everything we do, it works.

Third orientation is simply about geography. A training officer or manager escorts our recruit to every nook and cranny of the property—in uniform. Many reasons for this—evacuations, patrol techniques, and all that. It takes the mystique out of the guest-facing parts of the property to see where hallways and doors connect and to know shortcuts and hiding places. It also supports the team-building that I will speak of throughout this chapter.

Three orientations! My gosh, my heavens, my budget! Fear not. The first orientation is the mandate from the company, that is going to happen no matter what—and even though it is at your expense, it is justified on your payroll line and even authorized for overtime, I bet.

The departmental administrative orientation can be handled as soon as they are hired and may take no more than a couple of hours, but beware: One of the undeniable truths of hiring says that nobody remembers anything on their first day. It is just too much to absorb. That is why this orientation is good for day one, because we are just taking care of paperwork, issuance of tools, uniforms, and all that.

The third geographical orientation is day one of training. I explained that in detail in Chapter 3.

DEPLOYMENT

When I was hired into a mid-sized casino hotel in 1990 as a security officer, there were about 130 of us. Imagine a property about the size of a large department store with a couple of hotel towers and parking lot. It was really busy but not 130 officers busy. That is because we were not deployed effectively. I called this the “shotgun method of scheduling” and I vowed to get into management so I could fix it. We had a feudal class system where the half-dozen or so kings would sit on their thrones (not the managers, but the senior officers) and wave their hands in an indignant fashion over us slaves who did all the work. By “work” I do not mean the fun stuff like arrests and throwing people out. They still got to do that. I mean patrolling the garage in 20-degree weather, sitting at a post in the basement when the basement was closed, and things like that. Certainly, this happens in other large organizations, especially the para-military ones like we were. Most of us have wised up and gotten a bit better at leading such an organization.

I can imagine how this happened even though I was not there to witness its inception. There were a couple of serious lawsuits related to a couple of really bad things that happened to guests before my arrival. These things can happen in any hotel, so no sleight on anyone here, just the facts. During the lawsuits, experts opined that there were not enough security officers on the property to prevent the bad things. People were deposed, experts were consulted, and somewhere along the way they came up with a magic number of officers, that when deployed, prevented bad things from happening. This did not make sense then and it does not now, but it was the measurement of efficiency at the time. So one of the results of the really bad lawsuit was a drastic increase in manpower—130 officers. We were bumping into each other, not because of the number but because supervisors were told to maintain a minimum staffing level, without any regard to where to put them and what they should do. Thus, I dubbed it the shotgun method because every day I would come in and maybe five of us were assigned to the mandatory posts and the rest of us were told, "Hit the floor." There is a shotgun blast of security to the casino. It is effective when it strikes a target, but rarely strikes a target.

Keep your eyes peeled next time you are out shopping, and you will see "shotgun deployment" for yourself.

What we need here is a security plan, which is why I ran you through that early in Chapter 1. There, we calculated the number of officers needed based on posts and patrol areas. Most of the work is done; we just need to contend with some variables—volume, shifts, and other duties. I suggest that even if you have staff and a schedule, you do this exercise. You may find some areas to make your staff more efficient or cost-effective.

Start with your minimum staff by listing your posts (fixed and roving)—hotel patrol, outside patrol, common area patrol, other areas, dispatcher, lobby key check, nightclub, etc. Do this for every block of time in a 24-hour period and for each day of the week. You do not need to do it hourly unless your posts change every hour. It might be 4-hour blocks or 8-hour blocks. We do the blocks because some posts are not staffed all hours, such as the nightclub. You may also want to add roving officers based on guest volume. More people up and around might require more security during those hours.

I can always tell a schedule done by a manager or director as opposed to an hourly supervisor. Those of us who sit at a desk all day forget about things like breakers. Add to each block number a breaker for every 4, 6, or 8 posts depending on your total break time. (Six officers who get 30 minutes of break time in your 4-hour block will get about one breaker officer.) Also, decide if you want to add any extra staff for report writing, emergencies, administrative duties, covering call-offs, and so on.

Now that you have this spreadsheet, create 8-hour shifts (or 6- or 10-hour shifts if you prefer). Do not hesitate to use staggered start times if that is how your shifts work out. You should end up with variable staffing levels that change with need and volume rather than the shotgun. You may have even justified that dreaded 10-hour workday that you have been trying to pull off.

In the next section, we will work on days off.

Schedules

There are several ways to work out a schedule. I will show you an easy way to do it. Suppose you need six officers on the weekdays and eight on the weekends. Each officer works a 40-hour workweek with consecutive days off. We will work on just one shift to make it easy. You can change these numbers depending on how many you need on each day.

Take a piece of graph paper (or create a table in Word or Excel) and create a draft schedule as shown in Table 4.1. Days of the week go across the top (column header)

Table 4.1 Example of a Draft Schedule

Officer	Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	X	X					
2		X	X				
3			X	X			
4				X	X		
5					X	X	
6	X						X
7	X						X
8		X	X				
9				X	X		

and the rows are the positions or officers. You can use names or just numbers 1 through whatever for now. I made nine rows. Make several more if you are not sure how many positions you will need. I then start creating position schedules. Since everyone has consecutive days off, I start on Monday marking an "X" for each day off. Line 1 is off Monday and Tuesday, line 2 is off Tuesday and Wednesday, and so on. When I got to Saturday on line 6, I knew I probably would not have two officers off on Saturday, so I skipped and gave that line Sunday and Monday off. At that point, I did a quick count of each day (counting blank boxes in each column) to see what my officer count was for each day.

That quick count told me I was running about four each day and five on the weekends. Since my goal was six and eight, I was on the right track and just needed to add a few more positions with the days off evenly dispersed. The next three positions were added with different days off, giving nobody Saturday off. This schedule worked out almost perfect. I have six on weekdays, eight on Saturday, and seven on Sunday. If that is acceptable, great. To fill that spot on Sunday, I could use overtime, part-time, or hire one more position and over-staff on other days. If that works for your budget, I would do it, because there will be sick calls, vacations, and extra days off that will decrease much of that extra payroll.

This simple exercise can be expanded to any number of officers. Those who use the "shotgun" approach mentioned in the last section can do this scheduling method, only backward. Start with the number of officers you have in the left column, and then do the same process, filling in the days off as you go down the line until days off are equally dispersed.

Do your staff a favor and create a schedule that you can stick with and not change every week. I am sure you have a restaurant manager who creates a weekly schedule with split days off and does not tell his employees until the Friday before the week starts. This is not considerate of employees' lives and does not promote loyalty or positive morale. Inconsistent scheduling with split and different days off will not benefit the company either. You will have more sick calls (to get their consecutive days off), employees who are not properly rested, and in the extreme you may have those who will join unions to get better work conditions.

Minimum Staffing

You must make two decisions before you manage a staff of any size in security: (1) What is the minimum you need to keep everyone safe and secure? (2) That number should be based on the security plan, but discussed with upper management with a plan for

> Security on trial: See if you feel comfortable answering these questions after the scheduling section.
>
> 1. You had six persons scheduled for the property when my client was attacked. How did you come up with that number?
> 2. On Mondays, you normally have six officers, but on the Monday my client was attacked you had two sick calls, reducing your staff to four. How do you justify having only four officers?

WAGE STRUCTURE

Wages are the most important thing to your employees and your management. No matter how much someone loves their job, it is difficult to maintain a cheery attitude when you are worried about paying rent. I know all of us have been there because we all started as low-paid security officers. Am I right? Employees want wages to be higher and management wants them as low as they can be to increase profits. Whether you are establishing a new department and a new wage structure or need to modify your existing one, here are several elements of a good wage program.

Survey

Competitive wages are important to morale and vital to recruiting a competent staff. Before starting the survey, you need to determine with whom you will be comparing salaries. Like the Risk Assessment, we have to compare to the local market, the national market, and the industry in general. However, if you live in Houston, Texas, you should not expect to pay as much as in New York City.

A good HR department will do a wage survey for you, but you can probably do it easier yourself. Your colleagues at other properties should be more than willing to participate in a survey, especially if you share the results with them. A survey should be done once per year. Beware your “friends” at other properties. They will bend the facts a little to throw you off. Ask specific questions, not just “how much are you paying?” Get starting pay with no experience and then find out how much and when is the first increase, the top pay and the pay after one year. Be careful as they will throw in special duties that pay more or other positions.

Base Wage

Naturally, you would like to be at the top of the market in pay. This attracts better applicants (well, more applicants) and can promote longevity and morale. The survey will help you appeal to your boss for a competitive wage for your staff. Where you place—and where you want to be placed—in the survey is dependent upon several other factors. These include the amount and frequency of raises, training provided, experience required, specialized positions, benefit package, and the reputation of your organization.

Raises

Most companies provide a cost of living adjustment (COLA) and possibly a probationary increase. I recommend a structure based on experience and training. This recommendation is outlined later in this section. As for determining the base wage, you may want to start a bit below the highest payer, if you have a substantial probationary increase. Or, you might start highest if you have no such type of raise. Another consideration is if you pay more for armed officers, experienced officers, EMTs, etc.

Training

Providing compensated training is rare in our industry. If you provide it, then that is a benefit and should be included as such when you publicize an open position. When you calculate your starting wage, consider this paid training. (Lower starting pay is more attractive if you pay training and other hotels do not.) By the way, I would never recommend providing training without compensating the employee, but some organizations do it and get away with it.

Experience

Many businesses base the starting salary on experience or education. This is a double-edged sword. You may attract better candidates, but as mentioned earlier in the Hiring section, experience is not always a plus. If you do provide this added pay, your base pay should be lower than the competition. This goes the same if you offer pay right off the bat for those specialized positions mentioned previously.

Benefits

Human Resources will tell you that the benefits that the company provides are worth $4 per hour. If you provide these benefits and the other hotels do not, that is plenty of reason to have a lower base pay. If everyone has similar benefits, but you start them at four months and others start them at six months, for example, then you also have an advantage. Some companies have gone to day one benefits to attract applicants.

Reputation

Finally, the reputation of your department and your hotel may affect at what pay you start your officers. If you have an iconic brand name, or your security department has a reputation for being good to its employees, you can afford to start at a lower pay because your applicants are not drawn to you for money, but seek prestige. If I may boast here a bit, I dare say we had a reputation of being better-trained, better-equipped, and high on morale. We had applicants willing to take a three or four dollar cut in pay to come work for us. I cannot take credit for this success but I will say that I did everything in my power to maintain it. I wish I could have had the best pay and the best working conditions, but the former is difficult to control and the latter is harder to achieve.

Officer Development Program

I now propose to you the Officer Development Program (ODP). Although not unique, it is certainly an unusual way to organize, motivate, train, reward, and pay your officers. It was developed by officers for officers and I have seen it work quite successfully. In fact, when we developed it 20 years ago, it was hardly used by anyone, anywhere. Many companies caught on, however, and now it is common, even if it varies by location.

The premise of the ODP is to compensate officers based on their skills and to allow them to give those skills back to their fellow officers through training. The opposite is to have everyone make the same pay regardless of their contribution to the enterprise and to give them periodic raises across the board. That sounds like a union to me, so I want to be as far from that as I can.

This plan has multiple levels of officer, starting with entry-level and going up to supervisor trainee. The levels can be called 1 through 4, or perhaps trainee, corporal, etc.

An officer starts at the entry-level wage. (For the sake of this example, let us say $15 per hour.) To advance to the next level the trainee needs to meet a couple of requirements, such as field training, CPR, and whatever you expect in the first few months of employment. Once they meet the requirements, and probably a fixed amount of time on the job, they advance to the next level. Sounds easy, but it also sounds like a probationary period. Stay with me.

The next level is achieved similarly but with optional training such as report writing, bike patrol, or whatever. It is also another time period—I used six months.

The next level is a little more difficult. The required training may be that of a trainer or a dispatcher or an administrative clerk or whatever you deem to be more advanced.

The final level is that of a supervisor trainee. This is one who has been trained as a supervisor and is either waiting for promotion, filling in vacation and sick days for supervisors, or even one who was deemed not to be of supervisor material, but they still have the added training and are valuable even as an officer because of that training.

Each level has a time period so that you cannot become the highest level in two months. You have to do your time. Each level has a wage increase (say a dollar per hour). You can also develop a test for each level that proves proficiency. I tried this and it was a waste of time. Their supervisor can tell you if they are worthy of the advancement.

One more thing. After years of adjustments to this requirement, the procedure was that no increases were automatic. The officer was presented with the requirements and she had to "apply" for the increase when she was ready. We did not remind anyone. If you want the increase, simply fill out a simple form which states you have met requirement A, B, and C. Get it signed by your supervisor and send it up the chain. If your application is honest, you get the raise immediately.

Some people were just fine staying at level one. Maybe they were retired and wanted to take it easy, or they were drawing government benefits and did not want the extra income. Whatever the reason, maybe 10% of our people just stayed behind, and everyone was happy. The minimum months of service required to reach the next level and the percentage increase in wages, are variable and at your discretion based on your situation.

Remember that level increases are not promotions, but advances. This may be semantics, but your HR people are more likely to buy into this program if you are not creating layers of supervision. You are better off comparing levels to kitchen workers, who have been using levels for years. Their system is a little different, but the first level workers might be prep cooks, who then advance to line cooks, fry cooks, chefs, and so on. It is important that you do not create supervisors with these levels. Nobody gets to boss anyone else around based on their level.

My team, who collaborated with each other to create this system, was a proud group that valued their training, prestige, and status. They added a rank insignia, such as chevrons on the uniform. You also may want to adjust the wage increases to match your local wage survey. I also suggest a pay differential for those specialized positions mentioned previously.

Ideally, you will end up with staff that are smarter and more motivated to learn and share their knowledge with their co-workers. Morale should improve and sustain itself with the program. The best part of the ODP is your Level IIIs. These senior, more experienced, and better-trained officers now make up the bench strength for your next generation of supervisors and managers.

Another advantage to this program that I did not anticipate was when our parent corporation was restructuring and applied a wage freeze. Our increases did not stop because they were not considered cost of living or promotions. We were the only department increasing wages during that time.

A disadvantage I had was selling this to three or four different controllers. They understood it just fine, but they wanted to detail it. All of them wanted to forecast how many officers at each level we would have and limit those “positions.” I had to explain a couple things to them. (1) These are not positions. Everyone has the same job description, and they are all security officers. (Once again, stay away from union vernacular like “apprentice,” “journeyman.” These are not transferable to the union; they simply represent more training for the same position.) (2) I had to prove to them that we could not forecast the number of officers that would want the increase, earn the increase, or stay in that level for the forecast period. Plus, our turnover was high enough that a better paid officer was always on his way out when a lesser paid replacement was on her way in. That meant the cost of implementation of this system was minimal and the forecasting variables were insignificant and not worth the “position” tracking. (3) My goal was to have everyone achieve the highest level so I did not want to have to say, sorry but we have enough level IIIs—I cannot advance you.

After many years of tweaking, the above program remains to this day.

CONTRACT SECURITY

Having your own security staff is not for everyone. It is expensive and requires the additional layers of supervision. It is also difficult to develop the loyal culture. But small budgets, small staff, and often the lawyers dictate that it be that way. Here are some concerns to address for both sides so you can make informed decisions.

1. Reason #1: Training and experience.
   Contract security—or guards as they prefer to be called—originated at industrial properties like warehouses, factories, and vacant buildings. The risk at those venues is limited to asset loss and so the training is based on asset loss prevention. Hotels and other hospitality venues have an exponentially greater risk profile based on the people we invite to our properties. Most guard companies are trained in patrol techniques, property laws like burglary, and confronting intruders. They are not trained to assist an obese person who fell out of bed or finding a lost child or getting a drunk guest back to his room. Take CPR for instance. While most guard companies will train on CPR, their likelihood of using it is very low. In a hotel, depending on its size, we encounter unresponsive persons almost daily. When nightclubs, restaurants, pools, weddings are added, the variables training deficit becomes more apparent. This is not to say that guard companies cannot have the same training as you, but make sure they do or that you verify it. Finding a guard company that trains on these situations and all the other likely incidents that are encountered at your property, is expensive and unlikely.
2. Cost
   Frankly, running a proprietary training program is expensive. You need a full-time coordinator or manager. He or she needs some horsepower to back their skills (certifications, experience, etc.) so you may be sending her to classes. You need a few amenities like a classroom, AV equipment, file storage, props (floor mats, CPR dummies, etc.). And of course the labor dollars spent on training. It can be expensive. (I am going to show you how to build this program later.)

   You may be able to offset some of the cost with savings. If you are paying your guys $15/hour, the guard company is probably paying 12. The guard company is charging you 20. (These numbers are just for illustration). Your extra cost is $5/hour. Multiply that times an FTE (full-time equivalent) of 2,000 hours per year. So for every "guard" you have, it is costing you $10,000 per year more than your own folks. Can you train someone for that price? I think so. Of course there are benefits and other costs so it may work out to be less depending on your situation.
3. The thing they don't tell you. I found that people who did not make it through our application process were being hired at the guard company. Then we contract with the guard company and here comes the same guy we rejected to help protect our guests and assets. That is where I lose it. Now your risk people may tell you that is OK because that guard is not our responsibility. The guard company will pay if he screws up. See number 4 for my answer to that.
4. If you are going to contract with a guard company, check their contract. Most contracts will take responsibility only for negligence, which means if the guard totally botches something—maybe shoots someone—it is on them. That is a relief—not. If the guard makes a mistake or misinterprets something, it will be on you. For example, suppose you post a guard at the elevator bank to keep non-guests from going into the hotel. He inadvertently lets a non-guest into the hotel, who ends up doing bad things to a

guest. His company will say that it was not negligence, just a mistake that could have happened to anyone. That puts your company on the hook for something of which you had no control.

5. Finally, look at the culture you are trying to develop. Your own employees are loyal and dedicated to you and the company. They know your guests by name, they treat assets as if they were their own, and they discern violent intruders from lost souls better because they know their hotel. If you have an officer who strays from his training, you can correct it with training and discipline. If that happens with a contract guard, the most you can do is replace him.

The bottom line in the Proprietary vs. Contract question is, select the one that is right for you. Please make sure your concerns (or mine above) are addressed.

Having said that, I understand there are times you need to temporarily augment your force. I have been there as well so let me tell you what I have learned.

First, please check that contract and their insurance. Your risk people will require certain limits on insurance, and they can review your contract at the same time. You want them to be accountable for their actions, whether accidental or negligent.

Second, if you are mixing contract and proprietary security, I recommend segregating them by location and duties. If you have one of each dealing with a difficult person and it goes to use of force, it’s going to be ugly because of training. Give the contract folks the simple, non-confrontational, non-risk generating duties.

Third, establish post orders for the contract team. When I had some working for me, covering nightclub, I had to lay down some rules. We were short on bouncers, so I hired them as a supplement. This goes against all my recommendations, but we had to do it. So, we gave them a sheet of paper with rules on it. Those included simple things like tying your hair back, tucking in your shirt, and no hoodies. It also included hands off the patrons. Let security handle that. This is difficult to enforce but may help cover you if they do something out of line.

Finally, before hiring any company, look at their record. You can check them with the state agency that regulates them. See how they handle complaints and allegations against them. The brand name of your hotel is riding on this one.

You may find it less expensive, both operationally and legally, to pay overtime to your current staff for special events.

Security on Trial. Imagine these scenarios:

1. Contract guard is walking through the lobby and steps over a puddle of liquid. He informs the front desk to send a housekeeper. While he has his back turned, a guest slips in the puddle, breaking her hip.
2. Contract guard witnesses two men beating a young woman in your parking lot. He was given a strict hands-off policy so he calls the police and watches as the girl is taken away in a car driven by one of the men.

3. Contract guard is assigned to watch several gates at an event to make sure people do not get inside without paying. Not realizing the gates have to remain unlocked for evacuation reasons, he blocks them closed so nobody can get in.

Now put yourself in deposition mode and figure out your answers to questions that will come at you.

LEADERSHIP

I re-titled this section from "management" for two reasons. Many organizations have flattened out their organization chart to have fewer levels of management. I appreciate this concept as I always found no matter what position I was in, I preferred to have that direct relationship with the front line. When there were one or two levels between the boss and the troops, it created confusion and miscommunication much of the time. If you are running the department, you may have some alternatives to the hierarchy that you set. For example, you could have one director that is over all of the personnel. The assistant director, rather than falling into the chain of command, can be in charge of administration—purchasing, training, policy-writing, etc. The larger your organization, the more side positions you can have. This is just food for thought. The traditional chain of command works well also.

The second reason for changing the title of this section is that, like it or not, we are all leaders. There are many memes and one-liners floating around that define leadership in various meaningful ways, but the fact is, in the corporate world leaders are appointed, not elected. So if you are the one selected to lead, you better get on it. Fear not, there are plenty of tidbits throughout this book that will help you become a great leader. I had a boss tell me once that he was not necessarily the smartest or the most qualified, but he was in the driver's seat. We can all be leaders, but there can be only one driver.

The Hierarchy

I often interchange the term manager with supervisor. This is mainly because I think anyone who is in charge, is a manager. "I want to speak to a manager,"—all too familiar words heard in every service industry. Our guests know who is in charge and that is who will resolve their problems. "Supervisors" are not perceived the same way. So, my recommendation is to make managers out of everyone with responsibilities to answer that call for a manager. Supervisors, in my mind, are those training to be a manager.

In my world, I put a heap of responsibility on a manager and she deserves to be called one. Consider your operation. Do your managers have responsibility to evacuate the property during a fire or active shooter? Do they respond to those calls for a manager? Do they have resolution capabilities that officers do not have (comps, refunds, discounts, etc.)? Do they manage life and death situations? I know we are back to semantics, but those who make life-saving decisions should be called Managers.

Creating Managers

There seems to be two philosophies in hiring managers. One is to find someone with maturity and experience as a manager. Second, is to find intelligence and attitude within the ranks. I prefer to promote from within as it boosts morale by giving those who have paid their dues some hope for advancement. Bringing in someone from outside to lead a family and a team that have built a rapport and a culture, just seems counter intuitive. However, I do understand that sometimes there is simply no “bench strength” within the group or that fresh eyes are needed to pump the group.

Promoting from within, therefore, is not about experience because your staff of non-managers has no experience yet. Rather than experience, I look for attitude and intelligence. After all, I am NOT going to train this person how to handle situations. I will show them the ropes, so to speak where to find the paper clips, how to build a schedule and things like that. But you cannot teach someone how to handle an angry guest or manage a crime scene. You can provide them with resources and tools for resolving the issue, but scripts and talking points are shallow, in my opinion. Taking a guest complaint, for example, is handled differently depending on your style and your wits.

Responsibility

Any team or organization needs one person at the top to take responsibility. For the department, it is the director. For a shift or other group—depending on how the team is organized—it is the manager. This responsibility cannot be shared, so if the group is large, there may be supervisors running smaller teams that report to the manager. Several managers can report to a higher manager like an operations manager.

Responsibility provides for accountability, which means that each person has a job to do, ensures that it is done correctly, and is held accountable for it. The manager holds his or her officers accountable for their actions and is in turn accountable to his or her boss for his or her actions. Accountability includes job supervision, training, coaching, and discipline. It also provides for delegation.

Supervision

The difference between a supervisor and a manager is the level of responsibility. Supervision is also something that both managers and supervisors do. Because managers are responsible for the actions of those persons on their team, they need to oversee all of the work being performed by those persons. Other steps in the supervision process are discussed next, but first, we must observe. Managers tend to be caught up in administrative tasks, such as reports, schedules, and meetings. These are all important duties, but a good manager knows he cannot take responsibility for the performance of others if he does not witness it for himself. Guest interaction, technical duties, patrol techniques, and confrontational skills are a few of the skills that a manager should be observing for all his team members.

Training and Coaching

In my perfect world, managers are a crucial key to the entire structure. I rely on managers to represent me, the department, and the company to our guests. I also count on them to develop themselves and their personnel through training and coaching.

If you are fortunate enough to have an internal training program, keep in mind that it is really not separate from your operation. Once a trainee is released to the operations folks and her manager or supervisor, the training must continue. What I have found is managers tend to not only take the training that the officer has already had for granted, but they tend to ignore and even contradict the training she received. In other words, the trainee learns the right way to do something and then gets in the "real world" and is presented with an alternate procedure. This diminishes the training program.

Managers need to be supervised also to make sure they are following guidelines that are presented in training, rather than make up their own. They can and should present their alternatives to the trainer or director to change the training rather than re-teach the trainee.

Training does not conclude after initial training is complete. Officers (and managers) will be constantly learning as they encounter new situations. It is the manager's job to organize and conduct this training. Some of this education comes in the form of group meetings, such as briefings, pullout training, and scenarios. Other opportunities for developing officers come during and after each incident. As the officer is collecting evidence or witness statements, responding to a domestic disturbance, or after a medical call are all good times to evaluate and coach officers on their performance.

Delegation

Delegation is the process of passing responsibility to the lowest level where it can be satisfactorily handled. The objective of delegating tasks is not to get someone else to do your work. It is a way of training: not only the task, but to take responsibility. Newer supervisor/managers do not always get that last part. Some other obstacles to delegating are guilt, trust, time, and fear.

Whatever delegation makes you feel is irrelevant. It is a requirement of management and of leadership. You are cheating the company if you are doing a task that can be performed by someone making less money. And you are cheating the subordinate if you are not giving her a chance to broaden her skills and responsibility. I believe that a good leader delegates in order to get others to grow and develop beyond their comfort zone. Rather than taking all the work you do not want to do and piling it on your favorite assistant, try bringing in the one whom you feel is least likely to succeed at the task. Start by explaining the task, even demonstrating the task, and asking if they have any questions. Do not ask if they can accomplish the task, just provide a deadline, and offer your assistance where they need it.

When I was in sixth grade, there was a boy—the athletic sports guy who was always the team captain or the leader of whatever playground activity was occurring. There was another boy that I can only describe as a wimp. Not athletic. Not cool. One day a basketball game was picking up and the first boy, the captain, needed one more player. He grabbed the wimp and said, "Stand here under the basket." If you get the ball, just pass it to me. I was impressed as a basketball player was born that day. Looking back, I realize what a leader the captain was. He did not ask if the wimp could do it, or if he would do it. He nicely but firmly told him to just do it.

This is not to say that delegation is about forced assignation. I believe it is about delegating someone to do something they may not have known they can do. Ask your subordinates if they will do something, not if they are able to do something. You are more likely to get a positive response.

Managing Managers

> Nobody knows the rules better than you, Spock, but sometimes exceptions have to be made!
>
> *Star Trek, Into Darkness* Movie

It is not easy. There are managers who, through their arrogance, are either too bossy or too lazy. There are other managers who are quite the opposite of lazy, getting into everything, and doing all the tasks themselves. Neither of these manager types develops a team. There needs to be a balance of reining them in and directing their behavior.

Leaders in a management role can be everywhere at once and know everything that is going on. They will not be able to do this "global thinking" unless they free themselves of tasks that distract from paying attention. A manager who is doing a proper job is one who is everywhere at once, knows everything that is going on, and has a competent and well-trained staff. This is simple for a director to observe. Start by observing the activities of the team. Do they handle routine situations without assistance? Is the manager consulted or advised on the resolution of all situations? Is there chaos during an emergency or order? Next comes some questioning. As we will discuss in Chapter 9, the director should work alongside officers and ask them how their manager is doing. Finally, test the manager and hold him or her accountable. Randomly check logs and reports and see if the manager is informed. Observe an emergency, or create a mock emergency scenario, and watch the manager's participation. Managers can make your job easy or difficult, but it is up to you to hold them accountable.

How do you select your leaders? Arguably they select themselves. I have a couple of ideas for you that I learned along the way.

Do not pick another you. We already have one of those. Watch your team and not only who stands out, but who does everyone look up to? Do not worry if they have different ideas or work ethic or style than you. Maybe that is what is needed. Don't ever be offended or threatened by the next generation biting at your heels. They cannot take anything away from you, they simply want to bask in your glow, hoping to gather some meager tidbit of talent that you exude as you walk. Not really. I know I waited forever for my boss to get hit by a bus so I could take over. In fact, his own motto was "timing is everything." That is enough of my melancholy rambling.

I made a 180 change in the way I selected managers and supervisors—actually maybe 90 and 270 because I used a couple of techniques. His first security department I headed was a very proud, quasi-military group and they liked it that way. Managers were selected by…you guessed it…written tests and oral boards. When I became chief, I said OK you can all go through the process, but you and I, we all know who the next manager will be. It was an exercise that made them feel good. One time they had a young new guy that tested out of the park and that stupefied them. Anyway, that is not my recommendation. Do not promote in this manner.

After that, I started asking the current managers who should be promoted next. That was not as great as I thought. They were a bit threatened by the talented ones so they picked someone they could manipulate. Not so great either.

When I promoted my first training manager, I had about 12 interviews—all in house. (That is very important to me.) At the end of each interview, I asked each one: So, who do you think should get this job—besides yourself? It was unanimous. The same guy was picked by 12 out of 12. Easiest and best decision I ever made. He already had the respect of his staff and he turned out to be my adviser, assistant, and friend. Of course he was the best training manager I could imagine.

I noticed one day that one of the departments which employed mostly younger folks, like teenagers, did not make such a fuss about creating supervisors. It kind of reminded me of grade school when the teacher would just hand the keys to someone and say go unlock the ball box. The entire room sighed with the thought that the one with the keys had just been promoted to first vice admiral, or ball monitor or teacher's pet. Anyway, this department would find an energetic, bright 17-year-old, hand them the keys and say make sure everyone gets their breaks or whatever. If the kid choked, fine, we try another one tomorrow. It always seemed to work out well.

My mantra after that was "anyone can do my job; everyone gets a shot." So instead of promoting them, we put them into training and after a couple of weeks, or maybe the first day, you know if a star is born. They put on a suit and strap on those keys, and it's like they matured ten years.

Let's get back to you. Why do you aspire to be in charge? Or why did you? Do not give me any horse hockey about helping people and world peace. Think about the real reason you want that job. I will go first: When I was biting at the heels for my boss' job, it was because I thought it was prestigious and FUN! Yes fun. I did not know everything he did, but he walked around rubbing elbows with the big bosses, he knew every secret in the building, and though he never really looked like he was having fun, I imagined I would. I also dreamed of all the changes I would do in that position—changing policies, firing people, buying new equipment.

The point of my question is to make sure you do not lose sight of your dream. If you like meeting new people, do not stay in the office all day; if you like investigations, keep your nose in it. If you just like being the boss, that is fine also. Just keep making yourself a good role model so the good guys will want to have your job and be like you.

MAINTAINING MORALE

I have found that morale is a product of effective communication. In fact, one could argue that most things rely on communication to succeed. Those other things will be saved for later. Employees want to be informed. They want to know stuff before patrons. Security officers want to know before their co-workers, because that is one of the benefits of being in Security: Inside information.

There are a million ways to achieve this and improve on it, but here are a couple of random concepts to consider.

Open Door Policy—This is one of the most over-used catch phrases in the Corporate playbook. It is rare that someone takes advantage of it and by the time they do, the damage can be irreparable. I am not sure why anyone ever closes the door anyway, except in unusual circumstances. After all, we are not the CIA. What is the big deal? (The door to my office did not hinder sound anyway.) While your door is open, go the extra step to ensure your team feels comfortable entering without being embarrassed. Replace your two wooden chairs with a couch. Put the golf game or the football game on your TV. Invite your folks to come in and watch. I used to have a candy dish with Halloween-sized chocolates. Once the little squirrels figured out that I would not bite, they would come in and get one, sit down on the couch, and get social. How are the kids? How do you like your training officer? Did you get those new tires for your car? Whatever.

I had a colleague who also had the couch and when an employee went by, he would yell at them to come in. He would offer a joke or some sports talk. He acclimated most of his employees to stop by each day for some fun and serious talk. He knew more about his staff and resolved more issues than I even knew of.

The Middlemen—It is frustrating for a director or senior manager when information does not get passed all the way down the line. Reliance on the manager or supervisor often results in a letdown, when you go to the front-line employee and ask them what they know about situation X. Usually nothing. About halfway through my career, I started using email to communicate good, bad, exciting and dull news to the entire staff. (I guess email was invented about halfway in my career.) The managers, wanting to be the first to know, would run into my office and get the back story so they would have something unique to share. I would give them the opportunity to put their spin on it.

I believe another component of good morale is the feeling of doing something important or useful. I remember in our slow days of winter that the boredom consumed everyone. Complaining and sick calls went up while productivity went down. There are many things we do to combat this fatigue. We would rotate assignments and create a lot of busy work. Busy work would consist of finding all the burned-out lights on the property and other useful tasks. We also did a lot of training during those times.

Motivation and morale go hand in hand. I think the secret is to find out what motivates them, generally. We got a good idea of this in their interview and hopefully rounded it out in their training. Some of your people are socially gifted, meaning they like to talk. This can go well or poorly, depending how you harness it. Avoid putting them in employee areas or where there is another officer. They will distract others from their work. But if you put them at a guest entrance, thoroughfare, or elevator, they will chat up your guests and that is always a good thing. On the contrary, put your shy or introverted folks behind the scenes, looking for safety hazards, clearing fire exits, and so forth.

Empowerment

Employees who are treated like drones and expected to blindly follow orders will never reach any level higher than that of a guard force. I am hoping that you would rather have officers that make decisions, protect the property as if it were their own, and enjoy their work enough to pass that attitude on to guests and the bottom line. Empowerment, the brother of delegation, is a morale booster, a motivator, and a guest service tool.

One comprehensive way to experience the advantages of empowerment is to get officers involved in the decision-making processes of management. When you have some free time and you want to kick it up a notch, try this empowerment exercise on steroids. Assemble a cross-section of officers into a focus group to solve a problem or organize something for the department—new uniforms, a wage structure, recruitment, etc. Use a manager to facilitate (after they learn he process). If you think your managers are part of the problem, use a manager from another department. The objective of a focus group, in this application, is to solve problems, create new procedures, or address some specific issue. This is a step-by-step process that will certainly get you some positive results.

1. Select the group members. Take a good cross-section of age, experience, and schedules. Quiet or loud, it does not really matter as long as you think each person will be honest and reasonable. This is a great way to reward those who always make suggestions and those who tend to complain without base. Be sure they are volunteers and that you pay them for their time.
2. Outline the rules. Facilitator keeps the group on track so that the meeting does not become a gripe session, that everyone participates, and that the results are not outrageous. That is explained below. Meetings should be about an hour. Two-hour meetings become ineffective and tiring.
3. Start with an objective: "How to improve guest service," "Improve our training program," "Reduce turnover," etc. The group will tend to go off into tangents and start solving other problems. The facilitator will keep the group focused on this objective. (By the way, use one of those easel pads and write this stuff down and post it on the wall until the focus group is disbanded.)
4. Once the objective is set, brainstorm some ideas of what a perfect example of that objective would look like. For example, if your objective is an improved training

program, your next line might be: more classes, better instructors, variety of topics, etc.

5. Next, you describe your current reality. (Yes, we are working backward for a reason.) Your current reality is how your training program is now: no variety, too short-handed to use on shift, OT has been crushed, same instructor is monotonous, etc. Once this is done, you have a disparate pair of lists just begging to be resolved, but not yet.
6. One of the reasons for having a group (you could have done this yourself, so far) is to get a variety of ideas. At this point, it is good to send the group out to gather ideas. This serves the underlying purpose of including others that were not in the meeting and practicing effective communication. Homework should be assigned to update the rest of the team and get their ideas for whatever. Additionally, they could go to other resources, like other departments, other properties, the Internet, or wherever—depending on the subject.
7. The next meeting or two will be fun and productive. You may call it "Connect the dots." Put your current world list on one side and the Objective List on the other. The ideas that connect these two will appear obvious, but you may find that there are some new gems that were not considered. The facilitator needs to keep participants focused and away from outlandish or unreasonable initiatives.

I used this concept many times and I was always surprised at, not only the fresh ideas, but how company-centric they were as a group. For example, when we worked on morale, not one person mentioned more money or benefits. Most input was about prestige, professionalism, training, better resources, etc. The "backward" method helps this because it narrows down topics and ideas to relevant solutions instead of that "shotgun" approach that we have all tried in the past.

Other Morale Boosters

The following ideas came from those focus groups mentioned above as well as some other experiences.

Image

Everyone wants a positive image. The officer wants to look good, smart, effective, and professional. What a coincidence? That is what *we* want, right?

Let's start with uniforms. Uniforms are dependent on the type of business, and even geography. First, decide on the message your uniform is trying to convey based on the objectives of the department. A "high-class" hotel may want to present proper ladies and gentlemen that dress similar to the clientele and the other employees. A motel may need something more utilitarian. An amusement park may need a distinctive law-enforcement look to prevent criminal activity, relate to children, and provide visibility.

I suggest asking your employees what they want. What are they comfortable wearing? What do they think gets them the most respect? What uniform allows them to use their equipment more effectively?

Guards

What do your employees want to be called? This is a very big deal for most security officers. A guard is someone who stands by a door controlling access—at best; and a piece of metal that keeps the chain from falling off your bike—at worst. We expect much more from our officers than guarding, such as rational thinking, discretionary decisions, and some personality. This is a couple steps (at least) above a guard and your employees should be recognized for this skill. Try calling them "officers" and see how their morale and self-confidence improves. This is a big change for the rest of the organization as well. They will require some time to acclimate to this way of thinking. This morale booster costs you nothing except a little effort.

Recognition

Officers enjoy the satisfaction of doing a good job and solving problems for others. Most do not require financial reward, though that is nice, but love being recognized in front of their fellow employees. A memo on the board does not quite do it, though it is better than nothing. Try mentioning something an officer did well in your daily briefing or other meeting. Or take it a step further and have the officer explain what she did to everyone else and make it a training process. What could be more rewarding than having something that you did being used to train others? Whenever you get a letter or comment from a patron or other employee acknowledging the efforts of one of your officers, write the employee a thank you note. Hand-write it and throw in a gift card for coffee or a burger. Have the shift manager deliver it in person with his own thank you because it makes him look good. This is guaranteed to foster "Aw shucks" embarrassment all around. They will probably cowboy up, and toss it aside as "just doing my job, ma'am." I bet they will take it straight home to their significant other and gush through dinner. This is also low-cost and worth taking out of your own pocket, if necessary.

Proper Training and Equipment

These are very important to your officers. This improves their confidence and gives them more tools to help their guests and employees. Take a look at some of your equipment, especially the basics like radios, uniforms, and so forth. Spend the money to make them work correctly. Nothing is more frustrating, and likely to cause more damage, than radio batteries that are worn and do not hold a charge, dead spots when transmitting and receiving, worn uniforms, and anything else that does not work well. Your officers consider all of these things, especially the radios (and weapons if you use them) important to their safety, so take this issue seriously and ask them what they think. In the long run, you will save money because good equipment is usually better cared for than the bad stuff.

PATROL

Overall Property

With all of the technological advancements that have occurred, and will occur, we have not eliminated the need for humans in Security. Hospitality, especially, will require security officers indefinitely in the future. There are some things that machines cannot do, and that is what separates the hospitality industry from manufacturing, logistics, and other types. The security posture of the property also needs to be decided in advance of the deployment of the plan. The director and executive team has to decide if the property will have uniformed security, and if they want to be visible and highly aggressive or discreet and reactive. Generally, the hospitality industry tries to be open and inviting, so bollards, guard posts, cameras, fences, and restrictive signage go against that philosophy. This is not to say that those measures will not be deployed, if necessary, but they need to be justified. CPTED is one way the property and its management can decide to mitigate risk while maintaining that hospitable feeling for its guests.

One of the first things learned in law enforcement or the military is the concept of layered security. If you think you are not familiar with it, don't be so sure. Anything that is protected is protected in layers. Your home, for instance, likely has several layers of security. Obviously, there is a door with a lock. There probably is also lighting, a peephole, neighbors watching, a standoff area (lawn), white picket fence, a barking dog, and maybe an alarm. These are all layers of security. Our hotel uses layers as well, and we will be documenting these layers in the Security Plan.

Layers of security in the hospitality environment are—primarily—physical, technological, and human. Layers can be considered as concentric rings around the asset, such as fences and walls around a prison. Layers do not have to be physically concentric. Just as in the previous example of your own home, the dog and the alarm are not actually concentric to the house. They are simply another level of security.

A layer is anything that detects, delays, deters, or denies entry to the asset. Examples of layers used in the Security Plan are thus explained.

Physical Protection System

The widely accepted standard for defining these layers is called the Physical Protection System (PPS). The PPS is all these layers working together and though not every layer is relevant to all situations, it still relies on these components working together to achieve the final objective.

People

The first component of the PPS is people. Humans are not being replaced in the hospitality world, despite technology replacing some of the job functions. Because we are a people business and a soft target, we will always need people to provide the human touch and make some subjective decisions. Of course, if you are a techie, you have seen movies and TV shows that depict artificial intelligence hosting us at luxury resorts, but it never turns out well, does it?

Seriously, there are many functions for which we rely on our employees to do.

Greeters—This is one of the most important functions of any security system. Retailers use it and so do we in hospitality. Greeting is at the root of the concept of hospitality and separates a resort from the Department of Motor Vehicles or a prison. Greeting is also one of our layers of security. It identifies us as the authority on the property, signals to the visitor that he/she has been recognized and is the eyes and ears of the area in which he or she is assigned. In a nightclub the greeter is the Doorman. In an amusement park or theater, it may be ticket takers or an usher. Many companies assign other roles to this function, which is understandable, but not preferred as we do want our greeters to focus on the objective.

The greeter serves many purposes for security and the property. First and most obvious is the hospitable welcome one would hope to receive in any establishment. How are you? Welcome. May I help you find something? The other functions are a bit more discreet. One is to make eye contact with every person. The theory is that (generally) criminals want to remain invisible. When someone looks at them and says hello, they are instantly visible, recognizable, and memorable. This is not a 100% solution to shoplifting or any other crime; otherwise, we would have wiped it out by now. But it does have a deterrent effect. A second function of the greeter is to profile. A seasoned asset protection officer can spot a shoplifter (purse snatcher, prostitute, etc.) on first sight. Even without training, an officer knows what a "normal" guest looks like. At a minimum, he/she can pass the visual on to someone else to watch the individual. At best, there are some questions and observations that can identify a suspicious person. This is discussed more in Chapter 8. The other more obvious function is watching those who exit. We see this at the big wholesale stores and others where receipts are checked. We can easily apply this to the hotel or resort where we wish everyone a nice day and thank them for visiting.

Patrol Officers—This is different from a greeter but may have the same job title. Patrol officer's sole responsibility is to patrol a given area, watching for security threats, safety hazards, and providing a deterrent by their visible presence. Assigning them to parallel duties such as escorts, running errands, or taking reports divides their attention and takes away from their effectiveness. It is understandable that they may have these other duties, but there should be others that cover their area while so deployed.

Guards—For lack of a better word, a guard (in this context) is someone assigned to watch a particular thing, like a door or a valuable object. Again, dividing their attention is not recommended. If you have an officer assigned to watch a bank of elevators, and he/she is also given other duties such as writing a report, you must be willing to accept that: (1) the report will not be as good, and (2) whomever he was supposed to keep out of the elevators may get past him/her anyway.

Supervisors/Managers—my philosophy has always been that we hire employees to follow policies, and managers to break them. Life would go along just fine without a manager if there were never any exceptions to the rules. But life happens and on occasion, there will be a conflict between the rules and reality. The manager or supervisor has to make a decision to stick with the policy or make an exception. Remember that it is your policy. You can break it or change it anytime you want, if you can justify the reason.

Others—There are other humans that we rely on to be a layer of security even though they are not called security or trained as such. The person cleaning the bathroom is a deterrent, for example. It is less likely for a bad thing to occur if an employee is in the bathroom. Regular cleaning and maintenance of the restroom not only provides a deterrence, but when documented also provides some investigative use as well. Most of all, that documentation proves the presence of an employee and can reduce your liability. Apply this same logic all over your property. Parking attendants, valet drivers, landscapers, facilities, every employee is a layer of security. This does not mean they replace security officers, but they are a helpful addition to your efforts.

This does not only apply to criminal or violent activity, but also accidents. The more eyes looking for spills and other safety hazards, the better.

Deployment

Deployment includes where officers are needed, how many, and what their purpose is. Some hotels use the “shotgun” approach to staffing and deployment: Hire as many officers as the budget will allow and spread them around the property to provide as much visibility and coverage as possible. This approach is obviously lacking in efficiency or logic. Even if money is no object, the idea of providing security based on geography, rather than risk, may leave the property wasteful in one area and negligent in another.

For example, the retail area of a hotel property would need more of a physical presence during business hours than it does during times when the shops are closed. That is because the risks associated with a retail area change as the chance of robberies, shoplifting, violent crimes, and even accidents are reduced when customers are not present.

Similarly, the retail area may require less of a physical security presence than a nightclub when both are open for business. A nightclub generally has higher risk factors, such as intoxicated people, fights, and larger crowds. (The documented Risk Assessment for each area would exemplify and justify these variances in security posture.)

Waste would occur where officers are placed in these lower risk areas, especially where locked doors and gates or cameras might suffice. Negligence might apply when something happens in the nightclub and an officer is assigned to patrol other areas instead of the nightclub.

Using risk factors to determine staff deployment in the Security Plan is much more efficient, and easier to justify. Other factors besides risk need to be considered in placing bodies around the property. Image, guest service, and other duties of the officers are explained next.

In a hotel/casino, security officers do most of the moving of money. This is generally not because of the risk associated with theft, but because most casino regulations require a department independent of the casino to be the third party in a transaction to avoid collusion. This goes against the popular belief that the casino places all its security officers around the cage and the pits for protection. The casino actually has much more to lose from a guest being robbed in its parking garage than it does with a theft from a blackjack table.

Upscale hotels do not earn their reputations lightly. They appear to put all of their efforts into appearance and service—as we learned above, most service efforts. This type of property is not only reducing physical risk and protecting its assets, it is also protecting the reputation and image in which it has invested so much.

Conversely, a smaller hotel with few staff members might have no visible security because they are not concerned as much with their aesthetic image. The security budgets are understandably smaller, and it might assign its security to drive the company airport shuttle. Security does this function because they have a driver's license, can handle most off-property guest situations, and probably because they are the only employees not assigned to other duties. This is not an ideal use of Security, but sometimes it is a reality in the hospitality business.

These variables will have to be calculated into the Security Plan depending on the situation of the property and after the other risk factors have been addressed. To mitigate the risk factors into the Security Plan, take each area that was evaluated and decide if it needs an officer to mitigate it. The Risk Assessment in the preceding section was made either by area or by type of incident. Either way, the Security Plan is better segmented by area of the property. As each area is reviewed, determine if it needs a fixed post, if it is part of some type of patrol route, or if other tactics can be used to mitigate the risk.

Work Force

There is no widely accepted formula to calculate work force in a hotel. Various groups and individuals have tried to assign ratios, such as one officer per number of square feet, or per quantity of hotel rooms, or per amount of floors. This might work in a warehouse, factory, or office building, but not in a hotel. The variable is "people." It completely depends on the quantity and demographic of the guests, the neighborhood, and the region. A hotel attached to a theme park or a casino has entirely different staffing needs than a business hotel in a downtown city or in a rural agricultural community. It may be easier to determine staffing if you had a magic formula, but it would be more difficult to justify it later. This is why we did the Risk Assessment. The reality of a Security Plan is that you can justify and document all day long, but if your company does not allow that level of staffing, you will have to deal with it.

If you are having trouble justifying your staffing level, or you want to justify more, here are three suggestions for your overall staffing.

1. Hire as many as your budget will allow. If you already have an established staffing level and budget, you are unlikely to justify more. If you are starting with a new operation, check the properties around you or in your brand line and take the highest number.
2. Use your Security Plan. Add up your total posts and patrol areas figured into your security plan and hire enough to fill those positions. Do not forget breaks and supervisors. Also, consider how many you need to handle a major emergency like an evacuation. A large hotel needs several officers to clear all the rooms. Select the higher of this number and the number of posts.
3. Find an established precedent. Any hotel that has had to justify their staffing levels for a judge or jury has a good benchmark for people numbers. This is not only an accurate estimate but is already proved in court to be adequate. If you have been through this, consider it the silver lining of all those deposition hours. If you have not been through it, find a similar property that has and compare those numbers.

It will be extremely difficult to decrease security staffing once you set your number. This is perceived as taking away protection from guests. This leaves your guests more vulnerable and you more liable. If you must reduce staffing, take the staff away from noncritical areas such as supervision, administrative duties, or merchandise protection. Keep some sort of documentation when you make changes to your security plan like this. Up or down, justify your reasons so that if you have to explain it—or someone else does—it will be there.

> In 2005, a man walked into a shopping mall wearing a trench coat with a rifle and pistol underneath. He called 911 and told the operator he was about to commence shooting. He shot seven people and took four as hostages before being taken into police custody. One of the victim's families sued the mall for inadequate security. The plaintiff argued that the mall did not take even the most basic steps to protect its patrons—armed security or off-duty police, tracking of past crimes, public address system, and coordination with police to prevent attacks. The mall owners argued that the incident was not foreseeable and, therefore, not preventable. The court sided with the plaintiff that the incident was foreseeable, and the mall should have implemented procedures such as those argued above.

The "people factor" may be the most difficult to manage, so the hardest part is over. The other components of the PPS—Policies and technology—will be explained in their respective chapters. But there is still more to come of the humans on patrol.

5

Patrol

BASICS

If you have been following along, you know that the Physical Protection System (PPS), the standard by which we protect our assets, has three components. The Policies and the Tools components have their own chapters and the third one is Personnel. A quick recap of how the three components work together is a car. The driver is the human or personnel that keeps the car from crashing by driving safely and managing the other two components. The brakes, headlights, horn, alarm, and all the other gadgets make up the Tools or Resources component and the final leg of this triangle would be traffic laws, speed limits, road signs, etc.

I find this a good concept to understand when making the security plan, but also about many daily decisions. Back to the old example of Vehicle Burglaries in your parking lot: When finding a solution, we sometimes go with one or maybe two legs of the PPS, forgetting about the third. If you install some cameras and post signs reminding drivers to lock their vehicles, that only makes up two thirds of the PPS. Failing to add a human touch will be considered an error on your part, and possibly even negligent. Even if you do not have human security officers, there are other roles for people in your system, such as having someone watching video, or asking employees to be vigilant in the lot, or even extra police drive-bys.

Every time you have a situation where you are applying security, make sure you use the PPS. For this section, we will look at how our humans contribute to protection.

Prevention

Human Security Officers contribute to the PPS in a few ways, but mostly by being a visible deterrent. Though the chapter is called "Patrol" and this is the majority of the job, security does much more than just walk around deterring crime. In my opinion, officers are the foundation of the property culture. This concept is difficult to wrap your arms around, but officers (and other dedicated employees) can set the tone for guests and other employees as to what type of place it is, how people will be treated, the stance on misbehavior and so many positive things.

DOI: 10.4324/9781003037644-5

As an example, take a look at medium to large cities where police are spread thin and spend their shifts chasing calls, rarely catching up. Contrast that with a city or town that uses "beat cops" or some sort of dedicated, walking patrol (or bicycle) to concentrate on public interactions and preventive patrol rather than response to calls. The latter areas will have lower crime rates, better aesthetics, and improved "morale" if that can be measured publicly. Ironically, this concept goes back 100 years in our country and even further in England. Somewhere along the line, US policing turned responsive, for the most part, and were spread very thin. This was a catalyst for the growth of private security.

My Perception of the Recent History of Policing

After World War II, the nation experienced a huge growth spurt, both by capita and geographically. There was no way for police departments to keep up with the volume of all these suburbs and urban growth areas. Security, which had been mostly industrial in the 1950s, began to expand into those suburbs and other markets, including residential. The police, started to distance themselves from the community, and after realizing it, tried to get back to community policing. This spawned programs like D.A.R.E and neighborhood watch. Departments found that they could not effectively work prevention at the same time as response and apprehension. Security, during these times (~1980s) worked with police in some communities and were adversarial in others. Each entity considered crime prevention as their home turf.

Unfortunately, in the 1990s, police departments were experiencing increasing costs of benefits and pensions, and basically gave up on the preventative aspect of policing. Security filled in this gap easily and happily with private patrols, and an increase in paying customers. This time, police are mired in social policies, effectual becoming overpaid social workers. They cannot go back to face-to-face policing because they have no money, limited manpower, and decreased staff. Recently, some activist groups have protested police as being too heavy-handed and racist. These groups, at the time of this writing, seem to be influencing local governments to make even more cuts. In my opinion, this will force those needing their services to hire private security. This was partly evidenced during the 2020 summer riots when retail stores hired specialized security to guard their assets while police were forced to stand by.

What does this political grandstanding have to do with the book? It is to illustrate that: (1) we may not be able to rely on police to come solve our problems as much as we have, and (2) they are not necessarily going to come when you call, as they may be busy or under an order to stand down. These truths will be self-evident as we go forward.

In my opinion, financial and political pressures will further regress these departments back to a social construct. If there is anything positive about that, it is that security jobs will increase.

A Tale of Two Cities

I grew up in Southern California, doing some work for LAPD (and the Sheriff's Department). I was fascinated, and I still am, about the differences between the LAPD and NYPD (New York). NY has about 36,000 officers, which is 3.5 times that of LA, even though LA covers a fraction more land mass. The population served by LAPD is a bit less than half of NY City's, but the most baffling difference is that New York spends six dollars for every one dollar in Los Angeles.

I had not been to New York until about ten years before this book was published. On that trip and two subsequent trips, I solved my puzzle. There was a cop (often a pair) on just about every street corner, plaza, and subway entrance. It was amazing to me that they could lay down such a thick carpet of blue daily. Then I realized they had found it: The Secret Ingredient! If you pour more money and resources at something, it will come out as you like it. If you have more security officers, your hotel will be safer, and the guest relations will be stellar. All our problems are solved. We just need more money, right? Right? You are not buying this are you?

Well, the facts are that New York has a colorful history of brutality, corruption, and discrimination. The citizens of NY do not think that much of their protective force. As a guest of the city, I was underwhelmed that I saw them everywhere, yet was not engaged by any of them (had I been selling coffee…). Los Angeles, I am afraid, did not come out much better in my non-scientific comparison. Angelinos might love their cops—if they ever saw them. The only people that meet cops are gang bangers and those who cheer them on as they race by on a freeway chasing a suspect with three news choppers overhead.

Which city is better? Wait a minute! It depends on the objective. I do not know either department's objective, but I can guess. What is your objective? As we move forward, I will make a case for the culture—an environment where people feel safe, where incidents are reduced, and the company is successful. I will use the examples of New York and Los Angeles that it is not the size of your property or your budget, but your success in strategy, training, hiring, and having fun! Let's go!

Preventive Patrol

Preventative Patrol may be 99% of the job. It can be boring, mind-numbing, and difficult to manage properly. Security officers tend to look at patrol as a time spent waiting on something to happen. Managers, for the most part, ignore this or are oblivious to it, because it requires some work on their part to ensure the job is being done. First, we will look at the reasons for preventive patrol, then the ways to manage it.

Patrol officers perform what I call "Security Theater." That is not to say they are acting or misrepresenting their actions. By theater, I mean that many things they do, and the way they do them, are by design, meant to show guests, employees, and criminals that security is active and busy protecting personnel. Visibility is the primary objective of security officers. Being seen is a way of reassuring guests, deterring criminal activity, and documenting that a certain area is being watched. Visibility is the first reason for patrol.

While patrolling, officers need to use their senses—at least four of them—to detect safety issues and policy violations. (Note I did not say criminal activity.) They should be looking for lights out, fire extinguishers missing, trip and slip hazards, and anything else security related. The ears should be listening for unusual noises, someone screaming, glass breaking, etc. Most sniffers vary in ability, but officers should be able to smell smoke, burnt wiring, marijuana, and other bad smells. The sense of touch is used to check that doors are locked, picking up debris that creates a hazard, and other safety issues. The sense of taste does not belong in patrol activity, so we will leave it out. Seriously, an alert officer is one using four senses to observe.

Safety Hazards are important items to report and correct by security. There should be a process for documenting a safety concern and then seeing it through to resolution. A light out, for instance, should be reported to facilities (or whomever), documented by security, then checked on each subsequent patrol until it is fixed. Often, security is the only one noticing these types of hazards, especially behind the scenes, so it is important that they own it until it is no longer a Suspicious Activity covers a variety of things in a hotel, or any tourist venue. Since we have an open-to-the-public soft target, we cannot just eject intruders. We can, however, identify those that appear to be out-of-place based on their behavior. Everyone we encounter is suspicious until we understand what they are doing. Someone walking down a hotel hallway could be a hotel guest or someone looking for open rooms. When he pulls out a key and enters a room, he is no longer a concern. An employee carrying a box of lobster from the receiving area to his car is suspicious until you find out he is delivering it to a wedding being catered by the hotel—definitely an activity to be verified.

A specific reason in the hotel is to check doors and be aware of nefarious activity in the rooms. Unsecure doors are a common way for thieves and assailants to enter rooms. Checking for open doors is important in any size hotel.

Other hotel issues are described in Chapter 11.

Some tools and technology make the supervision of officers easier but cannot yet replace a supervisor. Officers do not necessarily understand, or care, why they need to be moving, detecting, and deterring malicious activity at all times.

My first recommendation is to train officers the context of why they are there. If you ask them on day one, why they are there, they will likely say, to keep everyone safe. This is a great answer, but when you ask them how we do that, they will not have a good answer. We also train officers poorly, teaching them how to respond to situations, but rarely how to just walk along and be observant. Explaining some of the things in the paragraphs above will help if you hold them accountable to it.

One of the tools to locate security personnel is using patrol tracking devices. These range from a simple stick that reads a tag at certain locations to GPS-equipped phones or devices that physically track officers' whereabouts. (This requires significant infrastructure upgrades). Officers can also simply note their locations patrolled on a pocket log or call them in to a dispatcher or operator. Management can get clever with patrol tracking also. I know of one manager who used to put a purse in a stairwell with his business card inside. He wrote for the finder to call him when found. He would buy the officer dinner or ice cream or something. You can also leave a vacant room open or a light out and see if they report it. Though there is no standard on frequency of patrol, I recommend every two hours. Two hours is the approximate amount of time for one officer to patrol one good-sized hotel tower. That time period might depend on other factors that we determine in our risk assessment.

Good old face-to-face supervision can hardly be replaced by anything. A supervisor who goes up in the hotel not only adds to the patrol, but he/she can see personally what is going on with their officer. The same logic and techniques can be applied to all areas of the hotel.

Posts

Every area of the property will have a committed officer on post, a regular patrol, or it will be part of some patrol route. As discussed throughout this book, some areas will have other layers of security as their primary protection, but we still must physically check every nook and cranny of the property on a regular basis. Any fixed post or patrol route is called a Post. As with everything else we have discussed, patrol and number of posts are scalable. A large hotel will have many posts and officers to patrol, while some smaller hotels may have few or none. Whether you have many or one, each area of the property must be checked regularly.

The threats and risks we have in the public areas get much more attention for good reason, but there are threats to the back of house, basement, and utility areas that need to be considered as well.

There was a hotel in my home city that had a faulty boiler. The boiler had modern safety features, which shut it down when it had a faulty valve. The technicians ordered new parts, but in the five days they waited, a related gas leak filled the basement with gas before they returned with the new parts. Had a regular patrol been assigned to check the basement, they would have smelled the leak and prevented the explosion that collapsed the first floor into the basement.

To make matters worse, as firefighters approached the building, a second explosion of gas that was trapped in the elevator shaft, broke glass in the adjacent building, and blew the firefighters across the lawn back to their truck.

Basement areas, boiler rooms, electrical closets, roofs, storage sheds, catwalks, offices, and walk-in refrigerators should be on some patrol schedule, even if it is once a day. Let your imagination run for just a minute as to what could happen in these areas. Some examples of things that happen in these unpatrolled areas are safety issues, such as leaks or cracks, unauthorized sleeping areas for employees, drug labs, sexual assault hiding places, hiding stolen property, and other illegal or risky activity. If you can think of it, someone else already has. Employees, who know Security may stop by at strange intervals, will not take the risk.

Post Types

A fixed post is a guard shack, a security podium, a desk, or someplace where an officer is assigned all the time. A modified fixed post might be one that is manned at certain times and left to regular patrol at others, such as at a swimming pool. Fixed posts are used for high-risk areas or others where the risk can only be reduced by having constant attention. Access control is the most common reason for a fixed post. Of course, modern technology allows for using remote cameras, card swipers, and a myriad of high-tech devices. The company and the Security Director use the Security Plan to decide which is better based on cost, effectiveness, and image. The cost of a technological solution can usually be justified with labor savings, but sometimes loses to the more subjective live human. Thus far, there is no technology to replace reasoning, evaluation, and the welcoming nature of a friendly face. We must keep in mind it is a hotel for leisure, not a storage site for nuclear weapons, so the hospitable human may be more appropriate even if more expensive.

Regular Patrol is an area that is part of a fixed route or group of posts that are visited by an officer on a regular basis. The frequency of the patrol might change from one round to another, but on average, it should remain constant. While the fixed post requires one person to cover it, the patrol point is one of several posts covered by one officer. So, once the determination is made to make it a patrol point, the next decision is how many points are needed and at what frequency to mitigate the risk. This is discussed further in Chapter 2. One floor of a hotel is an example of a patrol point. It would be inefficient to make a hotel floor a fixed post (unless a dignitary staying there increases the risk). However, one officer might patrol all the floors or a group of floors on a regular basis. This is called a patrol post.

Eliminate the term “Random Patrol” from your vocabulary, your strategy, and your daily operations. There is no such thing, and if there was, how would it be decided? Leave it up to humans and it will be subjectively weighted toward certain areas, leaving others deficient.

I experimented with this once in a large hotel tower. The procedure was to start at the roof and walk each floor in a zigzag pattern all the way to the bottom floor then start over. I felt this was a bad pattern as bad guys could wait for us to pass a floor and know it would be a while before we returned. So we asked the patrol officers to patrol the floors randomly, go wherever they want, just keep moving, and we would check the patrol tracking software to see what type of coverage we had. This did not work because they would find a way to go to the better areas, the prettiest housekeepers, the best air conditioning, and the nicest hiding places. We tried the experiment again by saying, try any pattern you want, just make sure all floors are covered. You can do even and odds, five high, five low, whatever you want. Most of them decided to stick to the old pattern of starting at the top. The lesson learned here is, set the pattern you want and do not leave it up to subjective reasoning or some floors will never see a uniform.

Another phrase I like to avoid is “short-handed.” I hear this in every security department I have ever visited. Once again, imagine yourself explaining why you were short-handed when my client was raped. Is it because you put money above the safety of your guests? There is no right answer. Get your staff and yourself accustomed to saying that you are properly staffed. Put yourself in the habit of explaining every decision you make while on the witness stand. You might just change your perspective.

What is the alternative to being short-handed? Your restaurant, and even Housekeeping can close sections when they do not have employees to man them. But it is not so easy for Security. We are responsible for the entire building, whether it is full or not. I recommend that you do everything reasonably possible to cover those vacations, sick calls, and vacancies. As a last resort, you can do like the restaurant and find out what floors are not being used. These floors still need to be checked for squatters and things like fire, but maybe not so much time on the floor. A quick check can be done of these areas while more time is spent where your guests are. This may work in the parking lot during slow season. See if you can close some areas. If you are in a snow country, this really saves time on plowing.

Post Orders

Post orders are a set of instructions for each post. (Remember that a post is a place or area that has an officer assigned to it.) Post orders are included in our Security Manual (Chapter 2) and are meant to be given to officers who work a post so that they know what their duties and responsibilities are.

Post orders should be written for every post, even if that post is not always manned or is sometimes combined with other posts. For example, you may have a patrol area that covers the perimeter, valet, lobby, and restaurant. That patrolling officer would adhere to the post orders for each of those posts. It is less complicated if your post orders are individual to each of those areas. There is no reason to get too lavish or long-winded when writing a post order. One page generally does it, and the format looks something like a job description—with bullet points. Start with a description of the post. There are several posts that are consistent in all hotels.

Do not expect that your post orders are going to be a reference for each officer, especially the proprietary folks that have been there a long time. They only need to read it once. If you have contract folks that turnover daily or regularly, this will be a big help for them to know what is going on.

Elevators

This is the only static post I recommend. About 20 years ago, we realized that crime in the hotel could be drastically reduced if we keep the bad guys out. This is not a new concept when you realize that elevators had floor restrictions from the beginning. Elevator attendants were the standard 100+ years ago. The mega resorts in Las Vegas started manning the elevator lobby in the early 1990s. When the huge hotels like Excalibur and MGM Grand were built, they found that lookie-loos from the strip would want to come in and take a look at the hotel hallways. The Las Vegas Hilton, which was the home to Elvis for so long, had an entire floor for his living quarters and though you could not access it without a key, they sure tried. The post kind of waned for a few years and then was brought back for the nighttime areas when prostitution is at its peak. Now, after October 1, an Industry Standard has formed where every elevator lobby has an officer checking room keys.

So many bad things can be prevented by having an officer at the elevators. Officer's duties are ostensibly to check room keys, but they have other observations to make while there. The first duty is to ensure guests get to their rooms safely. This means overly intoxicated persons should be monitored to make sure they can walk safely, find their room, and that they are not accompanied by a stalker.

Officers at the elevator should also watch for unauthorized items—if you have a weapons policy, or policies against things like stoves, microwaves, bicycles, gas cans, etc. This is the time and place to watch for them.

Your post orders should include checking a room key for every party. There will be complaints on both sides of this issue. One side will complain that their key was not checked and how can you keep people safe? The other side will say, you checked my key but not the people in front of me. You decide how you want to deal with this, but my preference is that I would rather have complaints that security did its job, rather than not doing anything.

If your hotel does not have the staff to maintain the elevator post, I recommend deputizing your other staff to watch elevators. For example, the front desk, if it is adjacent to the elevators, is an acceptable substitute as they know who belongs in the hotel and can challenge those that do not. If you are a traditional hotel with a doorman, you might consider whether you're putting your staff in the right place. If you were to put your doorman at the elevators, he could serve a dual role of welcoming and observing guests.

I also recommend securing other ingress points to the hotel. Stairs that let out onto the main floor should be locked so they allow exit only and no entry. On the rare occasion that a guest prefers the stairs to the elevator, have someone open it for them. On one particular assault case, a hotel in an urban neighborhood had two banks of elevators that were monitored by cameras, but three stairwells that were open to everyone from the main level. A guest took the elevator to his floor and was accosted by unknown persons in the hallway. He did not see his assailants. A review of elevator lobby video showed no one out of place or suspicious. Other cameras found a group of teenagers walking through the lobby laughing and engaging in horseplay. Unfortunately, those stairwells were not on camera. The criminal case was not solved, but the civil case showed that if the hotel had secured those stairwell doors, the assault would have been prevented.

You may be saying to yourself, keys are everywhere. I can easily find a key and use it to show security. You are correct. This is what is called a "layer" of security or defense and is not 100%. It keeps the honest folks honest—like the tourists just trying to see where Elvis slept. If you are fortunate enough to see the contents of a hooker's purse, you will find, down there with the Aqua Net, eye drops, extra pair of panties, and hair brush, keys for all the hotels in the area.

You can tighten this layer with a little cooperation from your hotel. Key cards can get expensive, especially if they have RFID (Radio Frequency Identification) chips in them, so the hotel is not going to go for a new print of keys every day. However, when they do order them, how about putting a different color background on them. Use the blue ones this week, yellow next week, and so on. Then the prostitute or bad guy has to collect more samples of keys and figure out what color you are on this week.

Too often, we take an opportunity like someone with the wrong key, and let it go. If someone has no key or the wrong key, we want to know who that is. What a great customer service gesture to say, hey they gave you the wrong color key. Let me take you over to the front desk and get the right key for you. Oh, you don't have time? Tell me what room you are in and I will have them delivered. Busted. If you let it go, you are just deferring the crime until later. (This is true for minors with fake IDs, but that is another chapter.)

HOTEL PATROL

In Chapter 11, I go into detail about activities and behaviors to look for in the hotel. This section will talk about how to patrol the hotel.

I set two hours as my recommendation for patrolling the floors of the hotel. That means someone passes every room every two hours. If you have ten rooms then someone passes those rooms in addition to their regular duties. In a 1,000 room resort you may have one or two security officers patrolling the hotel full time. Patrol of the hotel is straight forward. As mentioned above, we are using the four senses to find things that are out of place, unsafe, unusual, or "just don't look right" (JDLR). Some checks are mandatory as part of this process.

1. *Doors ajar*. Doors left open are really a safety problem for our guests and a liability for us. The risks are explained in Chapter 11. Someone needs to check every door on every patrol to ensure it is closed. It may have been left open by housekeeping, the guest (accidentally or intentionally), or it just did not close all the way. Document doors that are found open and the disposition (such as a guest getting ice).
2. *Exits*. Stairwells, halls, and doors should also be checked on every patrol. Guests and employees will abuse the fire exits because they appear to be unused pieces of real estate where they can smoke, sleep, or store roll-away beds. Once you allow one item in there, you will lose control of the space. Keep everyone out and the area clear. If you have an evacuation, it will not be pretty for you. If the fire inspector (or a guest who likes to call people) sees a stairwell blocked…
3. *Persons*. For some reason, most security people who patrol the hotel think they are working grave yard in a warehouse. They do not want to talk to anyone or see anyone. I am afraid that is too bad. We need to encourage our officers (or other persons checking hallways) to challenge people they see. By challenge, I mean, simply talk to them. How are you today? May I help you find your room? As explained in Chapter 11, this technique allows for some behavioral recognition and you may just prevent a room burglary—or worse.

I had a case once where three single ladies were staying in a small hotel. They stopped at the lobby bar for a drink and the bartender was flirting with one of them and he got some signals that meant to him he was going to get lucky later. After his shift, he went up to the hallway and sure enough, the room door was ajar. He went inside and found the inebriated woman asleep and proceeded to have non-consensual sex with her. The woman woke up and freaked out and reported the rape.

In the bartender's mind, he was invited there, and she gave consent earlier at the bar. This was a question for the criminal court. For the hotel, it raised many other questions. Is there a policy against fraternization? (No there was not.) Is there a policy against employees going to the hotel? Yes, there was, except, bartenders were expected to go through the halls nightly and pick up empty dishes from the hallway.

The guest swore that she locked the door, and the bartender swore that it was ajar. The case came down to whether the door closed automatically and whose responsibility it was to make sure the door locked on its own. From a security perspective, there are many things we can do to prevent this incident in the future.

Polices that are written and enforced are the easiest and maybe most important. Keeping strangers out of the halls and making sure doors are self-closing are also important. This incident would have been prevented if any one of these things had been done.

There are other areas where you might set up static posts, and many other patrol areas, but remember that guest safety is always first. Now we will look at some other areas and events within the hotel and how to secure them.

Combining Layers

Other ways to secure an area or reduce risk involve the use of hardware or some type of equipment, such as cameras or locks. In some ways, hardware—or technology—offers a better and cheaper option for a layer of security. Locks, doors, and fences are generally infallible and cannot be distracted or overwhelmed. They also do not offer any subjectivity, which makes humans the better choice in some instances. However, humans cost more and have to have days off, lunch breaks, and insurance benefits.

Fixed posts, regular patrol, and security systems are most often combined to provide the most secure environment. It is the security director's responsibility to determine the best combination and application to reduce risk in each area. The director's experience, education, and training come into play here, but here are some basics that anyone can follow in securing an area in the most efficient and effective way possible.

Begin with the simplest method of security possible—such as a door. Then add layers until the risk has been mitigated. As you evaluate each risk, decide which security measure will most effectively and inexpensively prevent it. That may include a combination of measures or multiple layers such as a lock and an alarm, or prickly shrubs and a camera. This requires knowledge of those measures and layers and the experience of knowing what works and what does not. Do not hesitate to consult with an expert if you are not sure about whether it will work. You will find some good suggestions of what works throughout this book.

Using the standard hotel room as an example, the first layer of security is the lock on the door. In the old days, this was the Security Plan and you would be finished. As we figured out that keys could be lost, stolen, or duplicated, another layer was added. The keylock was replaced with a magnetic keylock and most of those issues were alleviated. Dead bolts and secondary doorlocks were added so guests would feel safe from the intruding housekeeper or technologically advanced burglar. For most hotels, the Security Plan is finished with the doorlocks. If the Risk Assessment includes the chance of robbery or room invasion, the next cheapest security method is the peephole. There is still the risk of door pushers, stalking crimes, and other violent acts, so it may be necessary to add cameras in the hallways or elevators. The final layer to add is physical patrol. Adding layers to physical patrol is achieved by increasing the frequency all the way up to a standing post.

In 1974, a popular singer was staying at a chain motel in New York. A man entered her room through a sliding glass door that was locked but easily defeated by the assailant. The man put a knife to her throat and sexually assaulted her. She sued the motel for "inadequate security" (one of the first suits of its kind) and was awarded 2.5 million dollars plus loss of consortium for her husband. The motel had admitted to experiencing several prior burglaries through the sliding doors and that the locks needed upgrading.

This lawsuit set a precedent for hotels and motels worldwide and is the main reason why we currently have deadbolts, night latches, peepholes, and other security measures.

SUMMARY

The Security Plan is a justification for your policies, deployment, staffing, and all the neat gadgets you have acquired. You may never need to justify these to anyone, but you need to be prepared to explain why you spent this much money protecting this and that much money protecting that. The Security Plan keeps this process objective. For example, 20 years ago cameras were installed in elevators. That was seven directors ago and now your new hotel manager wants to know why we are spying on people in elevators. A Security Plan would explain to you and your new boss that a sexual assault had occurred in an elevator, and it was the hotel's intention to avoid a recurrence of a horrible crime.

You also may find yourself on the witness stand trying to explain why the previous security director did not put a lock on the fitness center when it was built last year, and a hotel guest was robbed. This is why you want to update your Risk Assessment and your Security Plan often and especially when you take over the responsibility for each. Each time you make a change to your plan—adding cameras, reducing workers, remodeling the nightclub—consider how it will affect your liability. Ask yourself if you will be able to justify this change to your boss, to a jury, or to your successor if something goes wrong. The format of the plan is not as important as the content. If you are not sure of your format, use the previously mentioned outline or the one for the Security manual in this book. As long as you can read it and use it to provide your justification, you will be fine.

You need to keep current on new technology, current events, industry standards, and market practices. This knowledge is needed to keep your Security Plan current. (See Chapter 9 on career improvement.) At the very least, subscribe to magazines and newsletters that provide this information to you. Track cases and case law on matters of security and hospitality. Attend as many local and national seminars and organizations as you can. You need to be the subject matter expert on hospitality security to adequately protect your business.

VIP Protection

As a proprietary Security Department, protecting celebrities, politicians, and executives hardly falls into the mission of protecting the company's assets. However, we all know that these individuals show up, sometimes announced, sometimes not, sometimes prepared with Security, sometimes not. Whichever way they present themselves to you, their presence will disrupt your business and create a threat in one way or another. So, on occasion it may become your duty to protect these people from themselves and from others.

The amount of special security details that involve personal protection depends on your property, obviously. It is still good to know the basics. Here are some things about personal protection that most textbooks will not tell you.

Celebrities and politicians have their own reasons for having personal security—and it is not always about fear of violence. It could be for prestige. It looks good, obviously, to have a couple of thugs accompanying you to your hotel or nightclub. Some simply want their privacy and do not want to be stopped for pictures or difficult questions or whatever (which I always found ironic that someone who worked so hard to be famous wants their privacy). One strange reason I have encountered is that their insurance (or their agent/manager) wanted it to protect their investment. A final reason for having bodyguards is to provide employment for a distant relative. None of these reasons align with yours, so you are already jumping hurdles before you start.

Even though this is going to be a huge drain on your resources and a lot of planning, your property management is just drooling at the thought of the free advertising and publicity they will get when Miss X graces your property. On the other side of that shiny coin is the publicity nobody wants—God forbid—if something happens to her on your property.

If the Secret Service or the military is involved (President, high-ranking military, etc.) you will not have much say in what they do. They will take over floors, kitchens, lobbies, parking, whatever they need. That is not a complaint, just a fact. They do know what they are doing, however, and you might learn something. Otherwise, you are not a casual observer. They will need your expertise to understand the layout, identify employees and guests and open doors. You will not have to worry about inconveniencing guests very much. They like a big buffer between their principal and your guests, so be prepared to close entire areas.

Normally, with the government, you will be notified a week or more ahead—depending on if it is an overnight or extended stay. The last few times I hosted a president, they had him stay on the airplane because it is just safer and less planning. The only advice I would offer for working with dignitary protection is cooperate as best you can. I have heard stories from these guys where the hotel or venue staff was downright hostile making their job even more difficult. There are other advantages to doing this right. You will network with some of those federal agencies that can work in your favor. They will tell their associates—and your boss—of your professionalism. Finally, it is your patriotic duty. Speaking of working with federal agencies…You may be surprised to know that there is no reimbursement from the government for security associated with a presidential visit. Even the city or county are not paid for providing traffic control and security. This has nothing to do with you, but it is interesting to know why there is sometimes contention among these guys.

I do not have the same regard for celebrity security. There are some talented professionals that do this for a living. They are skilled, thorough, and professional. They are the exceptions. My encounters with "bodyguards" are not always comforting. Like my observation about nightclub bouncers, these guys seem to be hired for their muscles, because they look good in sunglasses, or they are the principal's cousin (true story).

Entertainment security is covered in Chapter 10. Except for entertainment, you will likely not have any notice that Joe Famous is coming. His bodyguard will not advance the appearance or coordinate beforehand. In fact, many will not coordinate at all. They will drive up, takeover your valet, intimidate people out of their way, and cause a disruption to your business that is not worth it. Now, management may like having Joe Famous on the property, so you are stuck in the middle.

This may be a conversation to have with management before it happens, but you need to know what boundaries you can set, and which rules you will let them break. One of your biggest concerns will be if they are armed. Just think that through and play "what if…?"

In most cases, your department will be one layer of security (such as with the president). On the other hand, you may be the proprietary source of information to the personal team that needs to get around the property easily. With some would-be celebrities or newsmakers, they may not bring their own staff, which puts you on the spot. Finally, some security staff or bodyguards may be your biggest threat.

Planning for this event is straightforward—if you are the one doing it. If you were planning it, you would first conduct a Risk Assessment. List the possible threats and their likelihood. Then create a Security Plan. Document how each threat is mitigated. This is also called an Incident Action Plan. Then you must arrange these plans, such as crowd control for celebrities, personal protection for a rich executive (and his or her family), and so forth. It is helpful to have a small group of officers or managers go through some sort of executive protection training to provide expertise in these situations. You also can contract this service to professionals.

As with the president or a very famous person, he or she will have his or her own security and only need you to assist with access and travel through the property. In this case, assign a liaison from your staff to theirs to help this process run smoothly. Remember for whom you work. Your mission is to protect your company. The best way to do that is to collaborate with these people, as a negative incident on your property is not good for business.

Dispatch

To some properties, Dispatch is a function of communication, to others it is a room where systems are monitored, and to the rest of us it may be a method of gathering and documenting activities. Call it a Dispatch Office, a Command or Control Center, an Operations Center, or whatever. The function should be all the above. Dispatch must be scalable according to your operation. Some mega-resorts and amusement parks have dispatch centers that look like police call centers.

A 200-room hotel does not need a full-time person sitting in a room. Other employees can be deputized to monitor systems like camera alarms, boiler alarms, etc. While I certainly prefer and recommend security-trained personnel to work in and operate these systems, it is not always feasible, so do what you have to do.

I will talk more about cameras later, but it bears mentioning a couple times: Cameras and their monitoring systems have little value unless we are watching them live. If you put a camera on the back door and someone walks in, you will miss them. Ideally, someone is watching for the threat and the other is responding to investigate. Cameras that only record, only live up to about 30% of their potential. They are good for investigating after the incident only.

Communication

Dispatch, in this sense, is just like a police department or a taxi service. Calls are received, prioritized, and dispatched to your officers. In smaller facilities, your hotel phone operators or front desk personnel may do this. A large property may have several persons devoted to the dispatch function. This becomes a highly specialized function, requiring advanced training, multi-tasking and knowledge of the property. Many hotels and tourist venues provide training similar to 911 centers to do telephonic medical triage, phone etiquette, radio procedures and language, hostility de-escalation, and more. On top of all this, we often ask them to handle housekeeping or engineering calls as well as the functions listed next. Training and experience are highly encouraged for this position, as it is an expectation of service from your responding agencies as well as your guests.

System Monitoring

Because Dispatch is usually a constantly staffed, isolated room, it is the perfect place to monitor video systems, fire alarms, panic and intrusion alarms, access control systems, and even facility monitoring (HVAC: heat, ventilation, and air-conditioning; boilers; etc.). Some of these functions are explained in more detail in Chapter 12.

Documentation

What better position to log all our activities than the dispatcher? While you are answering routine and emergency phone calls, dispatching a dozen officers, watching 20 television screens, and answering alarms, why not write all this stuff down for us? There are computer-aided dispatch systems that make this job a bit easier, but it is still a huge task, although a vital one for your department.

Patrol Procedures

Many security officers are assigned to a post or sent out to “rove” or “randomly patrol” on their own without knowing what to look for. They may have had some training, but have they ever been told what exactly they are patrolling? I introduced post orders earlier which are the specific assignments or duties to be performed at a specific post. Later, we will also talk about certain situations and how to handle them.

As for patrol techniques, they can and should be discussed in the classroom setting, but you will need to devote some field time to these practices. Without a consistent, documented training process for patrol procedures, you are likely to end up with each officer doing his or her own thing. In my experience, there are three or four stereotypes of officers that you might encounter in your hiring and management career.

The Thinker stands at his post with a fixed gaze into the distance. He is making eye contact with no one, watching nothing, and probably thinking about his big date coming up or the poker game he lost last night.

The Anteater walks through the building looking at the floor. She is probably looking for money, but maybe she has poor eyesight, and the carpet is the only thing in focus. Perhaps she is thinking about her date with the Thinker. Each of these officers is working at about 50% because they are being seen, which is good, but they are seeing nothing.

The Rookie is walking through another part of the building, one hand on his shoulder microphone and the other on his radio volume control. His head is moving around in circles like a ship's radar. He stops each time someone says something on his radio because he cannot walk and listen simultaneously. He is so preoccupied trying to see everything that he is not seeing anything. If there is a guest looking for an elevator, he will never know it and has no time to stop anyway.

Finally, there is *Officer Cool.* He is so slick, walking through the building, that nobody dares try anything on his post. His John Wayne swagger leads him to every pretty girl in the building and he will make sure they get his undivided attention. Somebody needs to unlock the trash dock? Officer Cool will wait for Officer Rookie to answer that call because he has to keep his rhythm going.

These are exaggerations, but I see the same officers just about everywhere I go. Without established patrol procedures, you will get results like these and your staff will be operating at about 50%—being seen, receiving calls, but initiating nothing. Security officers need specific tasks to stay focused. They need to be looking for something. When you provide expectations for patrol, you can measure the results. Here are some examples of patrol techniques employed by effective officers. Use as many as your staff can handle.

Safety

Safety is one of the primary duties of security officers. Each department in your organization may or may not do safety inspections, so the security officer needs to incorporate this into his or her regular patrol. The obvious things to check are fire extinguishers, blocked access, broken equipment, water leaks, water spills, etc. More subtle things to check are locks and pressure gauges on wet standpipes, house phones, auto door closures, loose handrails, broken floor tiles, etc. Officers should be encouraged to use facilities that guests and employees use so they can be checked and properly patrolled.

A common defense to injury claims is the "open and obvious" doctrine. This means that if a hazard is open and obvious, there should be no fault on the property owner for injuries suffered in an accident. For example, a light pole in the middle of a parking lot is in the open and obvious, so if you run into it, it is your own fault. However, if there is no lighting in the parking lot and a pothole is obscured by darkness, a fall into the hole might be blamed on management. These observations are subjective, of course, which is why people go to court.

Part of a Risk Assessment is to inspect each area for hazards, both obvious and discrete, and take reasonable measures to prevent accidents around them. Light poles, although visible and obvious, sometimes have reflective tape at eye level or brightly painted poles around them just to be sure. Daily inspections of every area should be conducted to find new hazards, such as potholes, spills, or broken tiles, so that they can be repaired or marked to prevent injuries. Defense of these more-than-reasonable measures is much easier than admitting you were not aware of them.

Parking

After some time patrolling a parking lot, officers get bored and lazy and ultimately get tunnel vision. They turn into one of those 50% efficient officers. Cars start to look the same and a broken window or suspicious person are less likely to be noticed. Try assigning specific tasks to officers to force them to get that neck moving: counts of cars, checking for sleeping persons in vehicles, inspecting permits or license plates for parking authorization, and checking for abandoned vehicles. This is not busy work, but good supervision. I had a supervisor that used to hide a purse near a car or in a stairwell to see how long it would take an officer to find it. The officer who found it would get a reward. Others would compete and the result was a more thorough patrol.

Headcounts

As I mentioned previously, counting is a great way to ensure officers check every public area as well as make eye contact. Guests who see officers looking at every single guest assume that they are very diligent and are giving everyone their full attention. One of the men at my church used to walk up and down the aisles of pews, very slowly, looking at every parishioner. For several weeks, I thought he was some self-appointed church security officer. I finally realized he was performing a headcount. I don’t think he intended to look so vigilant, but I figured if anyone got out of line, he would be the one to deal with them. He was providing security and probably did not know it.

Purse Advisories

Most guests (not just the ones with purses) travel with a false sense of security. I think they feel that they are on vacation and they have left their personal security in our hands. This is evident by most guests’ carelessness in the most basic situations. People walk away from their luggage, leave their doors open, and forget to lock their cars—things they would never forget at home.

In casinos, nightclubs, restaurants, and other crowded venues, it is common for thieves of opportunity to patrol the area looking for unattended purses or easily distracted persons not holding their purse. It is amazing how easy it is to distract someone on one side, while another grabs the purse on the opposite side and leaves without being noticed. In restaurants, the purse always goes on the back of the chair or on the floor—easy pickins’. A great prevention effort is to have officers who notice the unattended purse remind the guest to hold it. Write this in your daily log to show how many crimes you prevented. This also guarantees your officer is doing more than wandering through the restaurant aimlessly. The careless guest is left with a comfortable feeling that this place really cares about safety.

Loiterers

Persons hanging out with no business are opportunists, vagrants, or both. Of course, we encourage our guests to hang out with lounges, sofas in the lobby, and benches scattered here and there. These are guests, they are welcome, and we are happy to have them. The loiterers are taking up space, making the environment look bad, and will not pass up an opportunity for theft if it presents itself. As we discuss in Behavioral Recognition, later in this chapter, these folks need to be challenged. We always start friendly because it may be a guest. Create a culture among your staff where guests are welcomed enthusiastically, and vagrants are expelled with equal exuberance.

Eye Contact

There is nothing as powerful as eye contact. A good hard look in the eye will comfort a guest and dissuade an undesirable. Remember, we looked for this trait during the recruitment process because you cannot train it. The officers who do it well enjoy it and will not be ones who give you 50%. Encourage this practice with everyone every time.

Greeting

The greeting is also part of that behavioral recognition and is just good customer service. Encourage officers to greet everyone within a certain proximity. I am not too fond of the retail stores that require that every customer be greeted because it does not seem genuine. However, if you can have a general policy that requires it, your staff will appear friendlier and your patrol more efficient.

Patrol Duties

This section looks at each area of the hotel property and examines the risks, threats, and other guest issues and how they can be mitigated or addressed through policies and security actions. Hotel policies require some collaboration between Security, Front Desk, Housekeeping, and other departments. Sometimes they may be the policies of one department or another and even enforced by any of these involved departments, but the common goal is security. The following recommendations are made with this in mind.

Room Entry

We could easily devote an entire chapter to this subject and still walk away from it confused and arguing. Therefore, our purpose here will be to keep the Security department out of trouble while still respecting the guest's privacy. There are many situations for hotel personnel to enter rooms. They should always either be business-related or for emergencies.

Probable cause and the Fourth Amendment are for police officers and crime investigations, so focus on common sense and ordinary business purposes. The scene in every cop show I have ever seen, where they get the landlord to open the door so they can find the incriminating evidence, is a violation of the fourth amendment. Here are some scenarios you may encounter and how to deal with them.

The housekeeper tells you that she saw a white powdery substance on the armoire while cleaning the room. The guest is out, and the housekeeper has already closed the door. Consider locking the room so that you can inquire when the guest returns as to the nature of the substance. It might be baby powder or an illicit substance. Your concern is that it might be a dangerous substance and you don't want your staff being subjected to it. The guest can convince you it is harmless, make it disappear, or you can ask the guest to leave for refusing to satisfy your safety concerns.

A security officer smells smoke coming from a particular room. You have knocked and received no response. There is a Do-Not-Disturb sign on the door. You can absolutely enter this room by whatever means necessary because you are concerned for the safety of the guests and hotel property.

A neighboring guest says she heard a child screaming from a room and it sounded like he was in distress. Now you hear nothing. Of course, you can enter this room after knocking and calling the room.

The front desk clerk says he heard two guests checking into a particular room talking about killing someone at a political speech the next day. There is no reason to enter the room, as there is no emergency in the room. This situation might be better handled by notifying the proper authorities.

The bell person says she has seen a female who continually brings different men to her room. She suspects the woman is a prostitute and is using the hotel room for this activity. Once again, we are not police officers, there is no emergency, and there is no business-related reason to speak to this guest about the accusation. Depending on your local police department's policy on prostitution, you may want to contact them.

A police detective contacts you and says that a guest in a particular room has set up a check-printing operation and is engaged in forgery crimes from the room. He asks that we find a reason to enter the room and verify if the equipment is there. This is a criminal matter and you acting as an agent of the police will not only violate the guest's rights but may nullify any evidence that comes from your warrantless search. Kindly remind the officer that he needs to follow his department's procedures and obtain a warrant.

The local fire department calls you and says they received a call from a relative of a guest in a certain room. They said they received a text message from the room occupant that he was going to take an overdose of pills to commit suicide. This is an emergency and entering the room is reasonable.

You find the above room empty, except for the guest's luggage, so you decide to search the drawers to make sure there are no weapons or drugs. This is violating the guest's privacy and is not an emergency. Do not search anyone's room without permission.

Note that we avoid acting as agents of the police and searching for criminal activity. Our concern is always safety.

Housekeeping

Most hotels have limited guests to three days in a room for no housekeeping service. There is no legal reason for this, but plenty of others. Rooms tend to stink after a while. Guests may be doing some illicit activity. The guest may be dead or ill. After October 1, almost every hotel changed this policy. (You may recall that the days leading up to October 1, the shooter turned his suite into the Alamo.) Now, hotels have either eliminated the Do-Not-Disturb sign (DND) or they warn the guest that we are still coming in each day, regardless of the sign. Housekeeping needs to be trained to report anything out of place or unusual on their daily inspections.

In 2011, a housekeeper at a New York Hotel made allegations against a guest that she was sexually assaulted in a room. This case received international attention because the alleged rapist was a French politician. The case was later dropped when prosecutors found discrepancies in the housekeeper's story.

This case famously shed light on the dangers our guest-room attendants face on an almost daily basis. It also exposed the risks our guests could face of being falsely accused just for being alone in a room with an employee.

Since 2011, Guest-room attendants, their unions, and the public have lobbied for panic buttons to keep the maids safe. Many hotels have bought in and some states and local jurisdictions have begun mandating the panic alarms in hotels. There are many other ways to enhance the security for our employees and guests and they are included in this chapter.

Housekeepers (GRAs) are threatened, attacked, harassed, and frightened more than you might suspect. As with any minority group, with a language barrier, management often takes these employees for granted. I spoke to many housekeepers in my days and was horrified at the stories they told, most of them funny, in retrospect, but many of them scary. If you are not worried about the well-being of your employees, failing to address these threats could get you in trouble with OSHA, The EEOC (Equal Employment Opportunity Commission), and any attorney that wants to make a case against your hotel for having a dangerous work environment.

In the technology Chapter 12, I mention the technology that has come about because of this new awareness. Whether you have those gadgets or not, you should have some basic policies and procedures to prevent situations that are dangerous to your staff.

Marijuana

Marijuana is a controversial substance, and its legality depends on your jurisdiction. (But the way things are going—this time tomorrow it could be different.) The Federal Government, as of lunch time on the day I wrote this, considers it controlled, and therefore illegal. Whether or not it is legal, the odor is offensive to most people and difficult to eradicate. An easy way to resolve this issue is to make the smoking of marijuana or any similar substance against hotel policy. When guests are caught smoking in a room, the options are eviction or the payment of a deep cleaning fee. The threat of calling the police and tying up resources is eliminated. Remember, it is not our job to enforce laws. As a hotel, our aversion to marijuana is not its legality, but its offense to our guests and the damage it causes to our carpet and drapes.

Service Animals

Laws on service animals are not very clear. Unfortunately, interpretation of HPPA (Healthcare Patient Portability Act) makes it illegal to ask a person about their disability that requires an animal. According to a 2011 interpretation of the law by the government, you can ask two questions to people with dogs (Yes, dogs are the only sanctioned service animals): (1) Is it a service animal? (2) What service does it provide? Apparently, these questions comply with ADA and also HPPA because you are not asking about the human's health. Of course, the riffraff that likes to take their pit bull with them on vacation know how to answer the two questions, so you have no recourse. (Though I will admit I kicked out a guy with a pit bull once.) (Bring the US attorney down here and see if he wants to prosecute me. But that is me.) Now, if an animal causes a disturbance, such as excessive barking, uncontrolled soiling, or biting persons, then you can absolutely have the owner remove the animal because the hazard trumps the need for the service.

As for other pets, this is a policy decision of the hotel and I am sure that carpet cleaning, damage to furniture, and excessive noise will be taken into consideration if animals are permitted in the hotel room.

Wheelchairs or Other Mobility Devices

This policy should be handled delicately as well. Like service dogs, there is no "National Organization for the Certification of People who Require Wheelchairs." If someone is riding in a wheelchair, it is best not to even inquire as to his or her need for the device. Just accommodate it. The exception, just like the animals, is if the device is a hazard. Riding a wheelchair on the escalator or speeding through your property on a Segway are hazardous activities. Use caution when dealing with these situations. A warning is more reasonable than kicking someone out on the first offense.

Parties in a Room

It is better to have a policy that prohibits excessive noise than one that prohibits having a good time. We want people to enjoy themselves and we even provide the ice. Parties, then, should not be forbidden. If there are ten people in a room and there are complaints from the neighbors after midnight, then that is something you do not want. A good policy is the Three Strikes Rule. First strike goes like this: "I see you are enjoying yourselves, but the noise is disturbing the other guests. You can go to the lounge downstairs, or perhaps call it a night." Second strike is sterner: "Folks, I asked you nicely the first time. Now I must insist that everyone except the registered guests leave immediately. If I have to come back here tonight, you will all have to leave." Depending on the cooperation of the guests, time of day, and type of party, you may only have two strikes (one warning), or even no warning. This is a discretionary call by the security or hotel manager.

Underage Drinkers

It is too common to see persons under 18 drinking in a room. It may be that an adult rented the room for them or the adult is actually hosting the party. This situation is full of ramifications and you do not want the responsibility of intoxicated minors. As soon as you enter the scene as the responsible adult, they are your responsibility, and you need that "monkey" off your back. If you do nothing, you are now contributing to their delinquency and guess whom the parents will go after when something bad happens? You need to notify the parents or police. Get one or the other there and document everything. If a minor does not want to stick around and wait for the police, hold on to them (more on minors later in this chapter). You are far more reasonable to make a good faith detention of intoxicated minors than you would be in letting them go on their own.

Domestic Fights

Next to parties, your most common disturbance in a hotel may be the domestic fight. These are difficult situations with which to deal, so keep it simple by keeping our objective in mind: protecting our assets. Police officers have extra concerns when dealing with these because they must enforce certain laws created just for domestic violence. We do not have that burden, so our response is simpler. First, remember safety for your staff. Make sure at least two officers respond to this type of call. (If you are not adequately staffed and trained, call the police, observe, and report.) Second, go to the room and listen for fighting, screaming, yelling, physical contact, etc. If nothing is heard, check with the reporting guest, and find out exactly what was heard. A phone call to the room may be in order before knocking: "This is hotel security. Can you please meet our officers at the door?"

The aggressor usually opens the door. Remember your intentions. You are checking that nobody is in danger and other guests are not disturbed. Inform the guest that neighbors reported a disturbance, and you need to make sure everyone is okay. You do not need to do any investigation. You are not going to enforce any laws or take anybody to jail. This will befriend you with both parties. Ask both parties if they want to call the police. You can ask the "victim" in private if you think necessary to get an accurate response, but if he or she is an adult they can decide for themselves. Yes, even if there are signs of a physical fight. Many security officers are under the mistaken impression that they have a duty to arrest or call the police if one party shows signs of a battery. With no police being requested, we just want the disturbance to cease immediately. If we have to come back to this room, all parties will be evicted, and the police may be called.

This call, and all disturbance calls, requires a follow-up. After terminating your conversation with the guest, stay near the room for a minute or two. If it starts back up again, that is your eviction right there. If all is quiet, wait about 15 minutes and return to the room to make sure it is still quiet. This is done for the safety of the guests, but also because if a disturbance continues after you have been there, the reporting guest and other neighbors are going to assume that you are taking no action and they will be very dissatisfied with their hotel stay. In fact, a phone call (not direct contact) with the reporting party is a good guest service. Let them know that everyone is okay, you gave the other guest a warning, and that they should call if they hear anything else. You may want to offer them a different room.

Cooking and Other Unsafe Practices

Many guests prefer to bring their own food and prepare it in the room. It is common to see guests "smuggle" in rice cookers, toasters, and even microwave ovens. Whether or not you provide these items or a full kitchen in the guest room, you should discourage guests from bringing and using these items. Safety hazards, such as overloaded electrical circuits, inadequate extension cords, and faulty heating elements, are a fire hazard. Guest rooms are not properly ventilated to deal with smoke and especially an open flame or accidental fire from burning the toast. Of course, the odor of cooking may be offensive to other guests and is difficult to get out of carpets, drapes, and linen.

I have seen guests use their rooms as a laboratory, a machine shop, and even a methamphetamine lab. These practices make for a difficult mess and involve chemicals and substances that might be toxic and are definitely offensive to other guests. Prohibit anything involving chemicals from tuning up bicycles to waxing surfboards. These odors would be a reason for security to enter a guest room without permission.

> Did you ever wonder why some hotels put a chocolate on the pillow at night for guests? It started with actor Cary Grant at a hotel in St. Louis Missouri. He was visiting there with his wife, but had his female "friend" staying in another room. In an attempt to seduce her, he laid a trail of chocolates from his penthouse parlor into the bedroom and onto the pillow. The manager of the hotel thought it was a nice touch, so he began putting chocolates on every guest's pillow when their bed was turned down. This caught on and now many luxury hotels do this.

Door Ajar

The most common hotel crime is burglary. Theft from rooms is not always an "inside" job as most guests think. It is usually a result of the guest leaving the door open and rarely by lock-picking or forced entry, as they will allege. You may have (and should have) spring hinges or door closers that automatically close a door that is opened more than 45 degrees. Guests still leave doors ajar accidentally when they leave the room. The closer may need adjustment, or the guest is walking out, holding the door for the rest of the family, or hesitating to make sure he has his keys, and the door closes and the latch hits the strike plate without catching. Housekeepers may be guilty of this as well, either accidentally leaving the door open or intentionally leaving it open so they do not need their key.

Door pushers are folks who cruise your hotel hallways looking for doors left ajar. The amateurs will see a door open, go in, grab what they can, and flee. The more refined burglars will work in teams. The scout walks the halls, maybe under the guise of sliding coupons under the door and leaves a signal for the actual thief. The signal might be to leave the coupon sticking out into the hallway, or a mark on the door. There may even be a third member of the team that picks up the stolen merchandise after the burglar leaves it behind that big potted plant in the elevator lobby or the vending machines.

There are three effective ways of dealing with these thieves. One is the key checkpoint at the elevator lobby on the main floor. This is not a foolproof method, but has its advantages. Two is Hotel Patrol. Security officers patrolling the hotel need to be on the lookout for doors left ajar and act accordingly to secure the room. Third is employee awareness. Housekeepers should be made aware of this problem and make sure they secure all doors and keep watch for guests leaving doors open. Housekeeping, Engineering, and Security should work together to inspect spring hinges regularly and at every opportunity to make sure they close at an acceptable opening.

In the early 1990s, a woman returning to her hotel room from a night on the town inadvertently left her room door open. As she entered, she let the door close, and it did not latch. Two men, who had followed her from the bar, saw that the door did not secure, entered her room, and raped and robbed her. The lawsuit that followed probed every aspect of security in the hotel. Door hinge springs were examined and compared to hinges in other hotels, security staffing in the hotel was scrutinized, overtime and call-off policies were examined, and minimum staffing for the entire property was criticized.

Besides having regular patrol that looks for open doors, a routine maintenance or inspection schedule of doors is recommended.

Welfare Check

Requests for Security to enter a room are numerous. The room may be locked from the inside and Housekeeping cannot enter. A relative may be unable to find or contact their loved one, or the police may have received a call. Call the room first just to be sure. This will cover you in case you walk in on someone in a compromised position. Take a witness (or a backup if it is a possibly dangerous situation like a suicide). Knock loudly and announce “Hotel Security.” Open the door and announce again. Keep announcing as you slowly enter. Remember why you entered the room and leave once you have concluded that there is no emergency. We have no right to open drawers or search luggage. Remember, it is reasonable to expect Security to enter a room to check on someone’s well-being, but not to search for contraband.

Some luxury hotels and cruise ships offer "turndown service" to their guests. The maid comes in late afternoon and preps the bed for sleeping (remove spread, turn down sheets, etc.), puts a chocolate on the pillow, and may bring ice or towels depending on the hotel. This is an added touch that increases guest satisfaction, GRA tips, and eliminates last-minute calls for towels and ice.

Security can benefit from this service as well. Though the housekeeper can only enter rooms without DND signs, they should be trained and told to report anything suspicious in the room. It is an extra chance to see inside the room after it has been rented. Security should not ask for a turndown service as it would appear that it is unreasonable since you do not do it for everyone.

Privacy

A guest's room is his castle. It really is. As far as the law is concerned, people are protected in a hotel room as they are in their house. That means you cannot just enter a room for no reason. In fact, it must be one of certain reasons.

Danger—Smelling fire, hearing gunshots, screams for help, etc.

Housekeeping—Guest has not answered phone or calls for service after a preset amount of time. The first time is not good enough. It has to be long enough where a reasonable person would be worried for the guest's safety.

Eviction—You already have a reason to remove the guest, such as the Three Strikes rule explained in this section.

Lock-out—Explained in this section.

Reasons you cannot enter a room are:

Police request—If the police are looking for someone and they think he is in that room, it requires a warrant and the police should not even ask.

Suspected criminal activity—You think a guest is printing bad checks. There is no danger to anyone. Call the police and let them figure it out.

Unknown Guest

The more guest rooms you have, the more chance there is for errors with reservations and check-ins. From time to time, the Front Desk will question if a certain room is occupied, where they put a certain guest, or why an unoccupied room has luggage or persons in it. The rack clerk or hotel manager will generally resolve this with a phone call and some research. On rare occasions, they may ask Security to enter a room to determine who is in there or to read the name on the luggage. As mentioned in the "Privacy" section, a guest's room is his castle and a hotel error is not reason enough to enter a room. Here are some policy suggestions to resolve this problem.

1. Determine your hotel's night privacy time: a period each night when you will not disturb a guest with phone calls or door knocks unless it is an emergency (9 p.m. to

8 a.m., for example). During this time, if the Front Desk asks you to bother a guest to determine his or her identity, remind them of this policy and leave the guest undisturbed until morning. The worst that will happen is someone gets a free night out of you. Otherwise, you disturb a sleeping guest, possibly lose a customer for life, and look like an idiot.

2. During business hours, start by asking Housekeeping. The Front Desk has likely done this already, but maybe they did not ask the actual maid on that floor. They may have seen the guest or belongings in the room.
3. Call the room before making contact. The Front Desk likely did this already, but security should always do this before entering a room.
4. Knock on the door. If someone is there, you certainly have the right to identify him or her. Remember, the person is probably not a criminal. Treat him or her like a valued guest.
5. Do not enter the room. If it is normal housekeeping hours, let the housekeeper enter or enter with him or her. Do not go through anyone's belongings. Looking at a luggage tag should suffice. If you cannot determine identity from anything in plain sight, leave the room with everything intact and lock the room. This will force the guest to call for assistance when he or she returns. At that time, the guest may just think the key is malfunctioning. Verify the person's identity, okay it with the Front Desk, and let the person in. No harm—no foul. Alternatively, you can tell the guest exactly what happened. That may make the hotel look inept, but most people would understand.
6. If it is not housekeeping hours (swing shift), and nobody answers, you do not have a legitimate reason to enter the room. Of course, you could enter the room to see if someone is incapacitated. Rather than doing that, it is safer to just lock the room and await the guest's return as mentioned previously. This beats walking in on Mr. Smith's collection of panty hose and sexy lingerie.

Room Inventories

It is common for the Front Desk to have you lock out a room in which the guest has not paid. This procedure, if done consistently, is harmless and painless. Generally, a guest is due to check out in the morning. Housekeeping will report to the Front Desk sometime before they go home that the room is still occupied. The Front Desk will generally wait until early evening, and if they have not heard from the guest they will ask Security to lock the room out.

This is best done with a witness. A second Security officer or even another hotel employee will suffice. Follow your room entry policy. One of three things will be apparent upon entering the room. It will be empty of personal belongings. In that case, it can be left as is and Housekeeping informed of its availability. If there is luggage or belongings, but no people, we generally lock the room. If there are people in the room, call the Front Desk for their advice. They will ask the guest to pay for another night, to leave as soon as possible, or apologize for a bookkeeping error made by the hotel.

The hotel, depending on the need for the room, will ask Security to remove the belongings from the room. This is called a room inventory. Room inventories should be done by two persons, properly documented, and the property secured. Lost and Found is the most logical place to secure these items, not at the Bell Desk where everyone has access to them. Belongings are kept for a reasonable amount of time—30, 60, or 90 days and then sold or given to charity. Keep in mind, the guest may be in the hospital, in jail, or dead. I have seen people return up to 6 months later. If a guest returns in the next day or two, the Front Desk will negotiate payment for the room and have you return the items to the guest. Have the guest sign for the items and retain this documentation.

Weapons

See the section on "Weapons Policies" in this chapter. Whatever the reason for the gun in the room, the response is generally the same. First, do not touch it. Leave it in place and lock the room. When the guest returns, explain your concern for having a firearm in plain sight in the room where the maid has access to it. Suggest (insist) that the gun be placed in the room safe, the hotel safe, your security firearms storage (yes, you should have one just for this situation), or their car. If they really want to keep it in their room, they should place it out of sight in their luggage. Remind them of your hotel policy that weapons may not be carried on the premises. (You can have a rule like this on private property.)

Make sure housekeepers know this policy, and always tell you about guns in rooms and never touch them. If you have some feeling or reason to believe that the gun is unlawful, stolen, or the carrier is a criminal, there is no harm in notifying the police. They can certainly run the name you give them, or come out and speak to the guest and inform him or her of local laws regarding firearms.

As for other weapons, such as knives, pepper spray, impact weapons, martial arts objects, and the like, treat them like guns and have the guest stow them for the safety of your staff.

Room Thefts

Guests will report missing property on a frequent basis. It is generally blamed on Housekeeping. (Internal investigations are discussed in Chapter 8.) There are two additional common explanations for these losses. They are both caused by guest error.

First is a theft by someone known to the guest—an "inside" job. Children, boyfriends, or roommates all occasionally steal from each other. Alternatively, it may be that they don't actually steal it at all, but pack it in the wrong place or lose it. It is difficult to control or know the actions of third parties, which is why you cannot accept blame for these losses. You can help them to prevent these losses by offering room safes or safe deposit boxes. Some jurisdictions actually require this as a condition of limiting your liability.

Many hotels issue safety tips with the room keys or in the room reminding guests not to leave their room receipt with their keys, not to be followed or fooled into giving out their room number, and so on.

The second common reason for loss in a room is the door pusher as described previously.

Violent Crimes

Throughout this section, we have looked at some of the problems that occur in a hotel. The most severe is violent crime. In fact, most of Chapters 1 and 2 and many other parts of this book are about preventing these incidents. If you are sued, it will likely be a result of an assault, robbery, or other violent act that you should have prevented. We have already looked at several measures that prevent crime in the hotel, such as locks, lighting, cameras, and certain policies. By far, the most important is human patrol. Your hotel should have some type of regular patrol, hopefully with an associated tracking system.

Security officers on patrol serve two purposes, as they do in other patrol areas. First is visibility. A known, visible, uniformed officer patrolling guest-room floors is a deterrent. I refer to this as "passive patrol" and half of the job. Second is active patrol. Active patrol is the action of that roaming officer looking for problems and acting upon them. This includes safety hazards, mechanical problems, and dangerous situations like smoke, screams for help, fights, etc. It also includes confronting strangers. This is really the heart of the entire hotel patrol: finding and challenging people in the halls. This is a way to catch door pushers, transients, and assailants lying in wait. A documented patrol of searching for and acting upon suspicious persons is one step closer to having adequate security.

In 2011, at an Atlantic City resort, an elderly couple was leaving their room to go to breakfast. They were confronted in the hall by two robbers who forced them back into the room at gunpoint. The woman escaped the room and ran down the stairs. The two robbers went back to their own room and barricaded themselves inside until police finally apprehended them.

It is impossible to prevent every incident like this in a hotel, but regular patrol, safety tips for guests, and even key inspections go a long way. (Note that the key inspection would not have prevented this crime because the suspects were actually hotel guests as well.)

Restrooms

Restrooms in common areas require a lot of attention from the Security Department. This is one of the few areas where we do not have cameras and our patrol of each facility is limited by the gender of our security officers. Threats we might see in our restrooms are graffiti, other vandalism, assaults, drug use and sales, and inappropriate sexual activity. (Some of these are also discussed in "Nightclubs" in Chapter 10.)

There are several tools we can use to defend against these threats:

Cameras cannot be used inside a restroom because there is an expectation of privacy there that cannot be invaded. One clever way of providing video coverage there is to mount cameras on the outside of the restrooms. This gives a clear image of those entering the restroom and not only enhances an investigation, but also acts as a visible deterrent to those who enter. Combined with regular patrol, the camera can be a valuable tool in catching vandals and other miscreants who think they are going unnoticed.

Patrol of the restrooms is essential whether you have cameras or not. Implement a well-documented regular patrol of EACH restroom. This patrol can be enhanced by your cleaning staff and your maintenance people by having them log their patrol of the restroom as well. Other staff members cannot replace uniformed security patrol, but they can certainly augment it. If you had an all-male security force, you would rely on these other departments to check the women's restroom for you. They can even be used to "clear" a restroom so a male officer can enter and do his own check.

Years ago, I was managing a hotel that catered to families. Lots of juveniles running around and we began having a problem with vandalism in the restrooms. Someone was etching our mirrors and occasionally marking up the walls. I pulled my team together and said there must be some way to put cameras in the bathrooms. NO! Maybe there is an alarm that detects etching. NO! We could put an attendant in there like some hotels do. NO!

What if we put the camera at the entrance to the bathroom? That will partially work but we would have to supplement that with frequent checks of the bathroom. Here is how it worked. We installed vandal-proof cameras at eye level at the entrance to every bathroom. By the time you noticed you were looking at a camera, it was too late—we had a facial picture of you. We also installed a panic button right near the camera to resolve a different problem.

One day, an attendant went into the men's room and it had been graffitied with a marker really bad. My security manager ran down to the camera room, rolled back the video and saw a teenage male with a backpack enter and leave the restroom at the specified time frame. (There were some other males but none that fit the profile.) The manager found the teenager elsewhere on property and interviewed him. After promising that he would not arrest him, he finally admitted to the crime. He was subsequently arrested and charged with the crime. (See the Investigations chapter about promises not kept.)

By the way, those cameras paid for themselves many times over in ways we did not expect. It turns out, everyone uses the restroom—even bad guys. Often before they commit a theft or other crime, they hit the head. We solved many crimes in other parts of the premises by having cameras at every restroom.

Restrooms near bars or other areas where young adults and older teens congregate are prone to drug use and drug sales. Officers should be aware of what this activity looks like from the outside. Some indicators of drug activity in a restroom are: the same person entering and leaving the restroom several times in a short period; "locals" who you notice day after day using your facilities; lookouts posted at the entrance; contraband hidden beneath counters and in toiletry receptacles; two persons in the same stall. The only way to prevent drug activity is constant, vigilant patrol. When doing patrols of the other common areas, the restrooms are a good place for officers to stop and observe while they rest their legs.

Your facilities experts already know most of the anti-vandalism methods available today, but it never hurts to make sure. There are many types of wall coverings that resist graffiti and damage. If you are seeing etching of mirrors, there is an inexpensive clear film that can be applied to the glass so that it can be removed if it becomes etched. Etching is either done with a sharp tool or an etching acid available at craft stores.

The Lobby

In almost every hotel in the world, the lobby is the main entrance to the entire complex. Generally, the lobby includes the Front Desk, Bell Desk, Concierge, maybe a lounge, guest-room elevators, and a connection to all of the other amenities offered on the property. This busy hub of the hotel probably does not see a fair share of violent incidents, crimes, or other undesirable activity because it is so well-patrolled by other employees and guests. However, because it is the main point of entry to the facility, it is where we can best apply our Behavioral Recognition skills. (See Behavioral Recognition later in this chapter.) It also becomes an important guest service and high visibility. Even if you do not think it necessary to have an officer in this area because of the low rate of incidents, remember that it is this area which allows guests (and perpetrators) to actually see your security posture for the first time. This first time needs to make a good impression.

Patrol of the lobby, as just mentioned, is primarily a guest service and “watching the front door” post. There are still many other things a security officer needs to be aware of in a common area. Safety hazards, unsecured doors, loiterers, and unattended property are some of the things a security officer will handle. These will be noted in your Post Orders for the Lobby. Post orders are discussed in detail at the beginning of this chapter.

Lost and Found

Guests leave objects behind very often in hotels. Administering a lost and found program can be quite daunting. Remember the objectives—Guest Service and Protect the Assets. I had a colleague that asked me once, why we do not just have a box behind the bar like everyone else. If only it were true. Lost and Found is an amenity that can grow beyond itself and take over your department like a weed. I am exaggerating, but I truly abhor it for many reasons that I will explain. Make sure your lost and found procedures keep these objectives in the forefront.

Administration

Decide who is responsible for the safeguarding of the merchandise and reuniting it with its owner. Security often handles this duty. This allows for a third party to be responsible rather than those who find the items. Housekeeping is another logical choice because they find the majority of the items and are already responsible for the guest rooms.

How will you find a trustworthy employee?

This position turns people into thieves. The temptation of uncounted merchandise is too great and the rationalization of "They think it's lost anyway" gets some of our formerly great employees into hot water. Organizational skills are also a must. I always hired those that were a little obsessive compulsive. They kept things in order, it was easier to note a missing item, and simple to find things.

Tracking

Depending on the size of your operation, you can use anything from a log book, to an electronic spreadsheet, to one of many software programs available for this purpose (see Chapter 12). Tracking information should include a description of the item, where it was found, date and time it was found, who found it, and where it is being stored. The disposition of the item should include person to whom it was returned, his or her address, ID (for verification), date and time it was returned, and whether it was returned to owner (RTO), given to finder, donated to charity, or sold.

Found Objects

The most important component of any transference of anything is to have an audit trail. This trail starts with the person finding the item. They need to begin the tracking process by completing a form or log with the item information mentioned previously. The policy needs to be clear on how they handle the item and where it is kept. Avoid allowing employees to keep items in their possession or to put them on maids' carts or storerooms where they are unsecured. Some hotels will have a runner available to transfer the item so the housekeeper can continue his or her duties.

Remember, the runner and the finder both need to be identified in the tracking process.

Valuables and Cash

These items should be handled differently to avoid loss. It is best to have two persons take possession and transfer the items to safekeeping. Cash, cameras, jewelry, and electronics should not be placed into storage where any one person has exclusive access to them. Regardless of how much you trust the lost and found custodian, that is where the suspicion will fall if these items come up missing. Consider a two-department safe at the Front Desk for valuables. This is called dual custody.

Storage

First, you will need to decide how long found items will be kept before they are disposed. Most guests will call the same day or within a week of losing an item to claim it. Thirty days is easy to organize and track if you have the storage space. You might want to save cash and valuables a bit longer just in case. Items should be organized by date found. Smaller items can be stored in something like a file cabinet and shelves in a storeroom will suffice for larger items that are left behind. (Many large hotels recover so many phone chargers that they do not even bother logging them.) Chargers can go into a separate area because probably they will not be claimed. They can be used as an amenity for those guests who forgot to bring theirs on vacation. The storage area should have access limited to one or certain persons. Items will come up missing from this area and you need to limit the list of those under suspicion. Having one person responsible for this function is best. Access afterhours can be achieved with a dual-custody or management key.

Do the Math

A 1,000-room hotel may average 10 to 50 found items per day. That is 300 to 1,500 items per month. If you have a mall, casino, nightclub, or other venue attached to your hotel, then that number could easily double. Do these calculations before configuring your storeroom.

Disposition of Items

About 25% of items will be claimed the same day. Another 25% will be claimed within about a week and they will have to be mailed. Some hotels charge for this service and some provide it as an amenity. Shipping supplies and postage add up, but it should not cost a large hotel more than about $3,000 per year. You need a policy for this: who does it, and how addresses are verified. I recommend *not* blind-mailing items to the address on the registration or even calling the guest to claim the items. The address could be incorrect and either the item will be returned or you will mail it to the wrong person. Calling the guest could get a husband in trouble with his wife—or worse. You will have to be reactive on this matter and avoid complaints.

The other half of your inventory is going to be unclaimed items. You need another management policy decision here. You can donate them to charity, sell them for profit, sell them to employees, or let the employee who found it keep it. All of these options are very time-consuming and you will need to decide whether each one is worth the return. Donating to charity is a worthy cause and might be a tax write-off. Selling items on an auction or classified Web site might be lucrative but may not be worth the labor involved. An employee rummage sale is good for morale, but also a lot of time and labor to organize. The finder will want some of the items. This encourages the employee to turn items in rather than stealing them, but it does not eliminate the theft problem.

SECURITY MEASURES

Consider what follows as your toolbox. Each of the tools has a specific use and may be combined with other tools to create multiple layers of Security. Not every tool applies to every venue, and some may not fit into your Security Plan, your budget, or your management style. However, you may find some that you did not consider before. You may employ all of them or some of them in combinations, and possibly others of your own not described here.

Search Stations

We do not normally associate personal and bag searches with hospitality, but more and more we are seeing this type of access control at our facilities. Common applications are parties or concerts of a certain demographic and VIP events. If you pick and choose which events have their guests searched, make sure it is for good reason. For example, if you search people going into a rap concert, but not a country/western concert, it will appear discriminatory. However, if prior incidents have been associated with a certain band or singer, that gives you enough justification to search those attendees.

If you are going to set up a search station, you are taking on a substantial responsibility. The search gives guests the impression that they are safe from weapons in the event. Here are some considerations for which you need a policy and training.

- A woman wearing skin-tight spandex, where a weapon could be seen, does not need to be searched.
- Provide signs of what items are prohibited and for what items you are searching.
- A policy for prohibited items such as lighters or pocketknives.
- A policy for handling contraband, such as drugs.
- Camera coverage and at least one witness to all searches.
- Train search staff on what they are looking for, what to do if they find it, maintaining a courteous attitude, and how to avoid inappropriate comments and touching.
- Do not limit the search to large bags. If you are going to search, search every person and his or her belongings.
- Do not use physical (touching) searches. This will cause more problems than you want. Use handheld metal detectors.
- Do not empty purses, bags, or pockets. Make a visual check with gloves.
- Do not put your hands into pockets or purses. This will avoid allegations of impropriety and theft.
- Do not allow exceptions to search. VIPs, special guests, small children, and little old ladies all get the same search. Discrimination or “profiling” allegations are the last thing you want.

A policy for bottles, empty or alcohol: Bottles should be prohibited for safety; alcohol, for over-intoxication and un-monitored consumption.

In 2010, a man at a nightclub noticed some guests being pat-searched and wanded with a metal detector and others being allowed to enter through another door with no Security measures. During the event, the man was shot by someone who entered through the unsecured entrance. The shooting victim successfully sued the venue for negligence for not following its own admissions policies.

It is important for a Security Plan to be consistently created and implemented so that all persons are treated equally, and all risks are mitigated. The second entrance in this case may have been for VIP or known guests, but as this incident proves, it was not a successful practice to treat the two sets of guests differently.

Arrests

As mentioned elsewhere in this book, arresting an offender is your very worst option, so it should be your very last resort. There are a couple of other options for dealing with criminals that are less dangerous, less expensive, and less time-consuming.

Refuse Service

The theme of this book is prevention and the easiest way to deal with problem people is to prevent them from entering your property in the first place. One of the greatest advantages of private security in private enterprise is to refuse service to persons who you deem undesirable to your business. Within your behavioral recognition layer, when someone who will potentially cause trouble is identified, he or she can simply be denied entry. This may include known troublemakers or criminals, ex-employees, or persons who are perceived as being a potential problem. This is one of our greatest tools. We do not need a reason, any evidence, or permission from anyone. We do not even need a sign. Of course, you cannot discriminate—refusing entry to blacks, women, or short persons—but you can refuse service to someone who stinks, who is smoking, or who is playing their music too loud. Keep in mind behavior, not appearance.

In the past five years or so, several court cases evolved from businesses refusing to provide wedding cakes—among other products and services—to gay couples. Plaintiffs argued that equal rights protected them from discrimination. Defendants maintained that religious beliefs prohibited recognizing gay marriage, citing various bible verses. The courts sided with plaintiffs in almost every case and the Supreme Court refused to hear any of them.

The takeaway is that you can still reserve the right to refuse service, except when the refusal is to someone from a protected class.

Trespassing

The trespass law is one of the most useful tools in our arsenal. States differ in their elements of this crime, but most put trespassing into three parts. The first one relies on posted signs, “No Trespassing,” which is not conducive to our open environment. The second part is entering a property after being warned not to enter. This is like the posted sign, except we specifically and verbally warn a certain person not to enter. When they ignore our warning, they are trespassing. This is commonly called an “86” and like the refusal of service, requires no legal reason. You can “trespass” former employees, persons who cause a disturbance, or anyone who you think might have committed a crime. Isn’t this a great tool? Just like your own living room, you require no reason. However, for your own sake, you should have policies and criteria on why you 86 people so you can defend these decisions to your boss or your lawyers.

The advantage of trespassing rather than arresting is that you do not need to prove a crime, but it provides the same result. Your job to protect the assets means keeping criminals out. Excluding them from your property keeps criminals out just as well as arresting them, right? In fact, arresting someone does not exclude him or her from returning after he or she gets out of jail.

The third part of trespassing is refusing to leave. Suppose you have someone creating a disturbance. You could try to arrest him for disturbing the peace, which is very difficult to prove and requires testifying witnesses. On the other hand, you can tell him to leave and if he refuses, he is trespassing. The law generally requires one warning, along with the consequences of refusal (arrest). This is a legally stronger arrest and does not involve other customers. Although it is not required, you should use another security witness and give more than one public warning. For example, holding a first, second, and third finger in the air tells the suspect, nearby guests, Security, and the cameras that you are being reasonable and clear in your warnings to leave.

Last Resort

Arrests cause injury, look bad to everyone, and open you up to false arrest, excessive force, and other legal issues. Less serious, but still troublesome, is the drain on work force, payroll, and lack of security in the rest of the property. Then there is the time taken by the police, jail overcrowding, and so on.

However, sometimes there is no other choice but to make an arrest. Most jurisdictions allow a private person to make a misdemeanor arrest committed in their presence and a felony arrest when reasonable cause exists. Those same laws generally require Security to turn over the arrestee to a police officer. This requires some procedures, equipment, training, and space. Here are some examples of procedures to have in place for when (not if) you make an arrest.

Procedures

When possible, a supervisor should make the decision to make the arrest.

Officers should use company "use of force" policies, approved restraint and compliance methods, and company approved or provided equipment (handcuffs).

For guest and officer safety, two officers should remove a handcuffed person from public view and take him to a dedicated holding area immediately. At least one officer should physically hold the arrestee to prevent injury from fall and to prevent escape. Once you have arrested a person, they are in your care, custody and control, which is legal-speak for: anything that happens to him is your fault. This includes slip and falls, injuries, and even illness.

Once arrest is complete, all force is suspended except that force necessary to transfer the subject to the holding area. Though it is "legal" to use whatever force is necessary to overcome his resistance, I learned the hard way that it is better to just "sit" on him where he was arrested until police arrive. This saves injury and the perception that you are using too much force if he is resisting nothing. This would include disabled persons in wheelchairs, with crutches, etc. Imagine a person with a bad back falling down in your custody.

The holding area should be a secure room, away from the public, audio and video recorded, with a bench or chair that is secured to the floor and with a locking seat belt to prevent escape. The holding room should be inspected before and after every incident to prevent hidden weapons and contraband.

A search is made for weapons for officer safety only. Do not search for drugs, stolen property, or identification. The police will do that. Remember that the room is recorded, so keep unofficial antics and dialog to a minimum. Do not allow eating, smoking, or phone calls by the arrestee. The police are responsible for this and will decide what is necessary.

Do not allow a restroom break unless the police are extremely long in arriving. Have a procedure in place for this in case you need it.

Have procedures developed for releasing a subject: one for releasing after a bad arrest and one for releasing if the police are not there within a certain time. Discuss this with your counsel. In my opinion, if you make a bad arrest, you have violated someone's rights and should correct it immediately, so you should at least be reasonable and release the subject immediately. The old line of thinking was to hold the subject until police arrived and hope for a miracle. If you release the subject and apologize for the inconvenience, you at least appear on video to be reasonable and not trying to do harm intentionally. The lawsuit is going to include false imprisonment and five minutes is certainly better than one hour.

If you are releasing a subject because the police cannot respond (a citywide emergency for example), make that call to the police in the room where it is being recorded. Tell the subject on video why you are releasing him or her, that you will still make a report to the police, and he or she may still be subject to arrest later.

In conclusion, make arrests a last resort. If you are going to deprive someone of his or her liberty, make sure it is lawful and that you can prove it. Be sure to document every step of the arrest and record and save as much video as possible to protect your lawful actions.

Video Patrol

Video patrol is a technique perfected by casino surveillance experts. Casinos and other venues that use cameras to prevent loss, such as retail outlets, are quite good at using cameras to observe, record, and apprehend criminals of all types. The basics included below are a good foundation for your own officers to enhance their skills and increase your effectiveness with camera systems.

Just like human patrols, surveillance officers use patrol routes for cameras as well. Routes are areas visible to cameras that can be "patrolled" electronically. Establish these patrol routes based on prior incidents, criticality of loss, and your risk assessment. Camera patrols should be documented and the documents reviewed to ensure no area is being overlooked or neglected. Routes also keep your officers focused and productive, rather than engaged in inefficient, aimless camera patrolling.

See Chapter 12 for monitor positioning. During routine patrol, officers should observe the following:

Guest behavior—This is more recognition. Do they look like guests? Are they acting like guests? Is there any suspicious behavior or suspicious items in their possession?

Employee behavior—Are they in their proper area? Engaged in normal work duties? Acting suspicious? Carrying anything suspicious or out of place? Is Security doing its job?

Property—Are doors closed and secure? Proper lighting? Any visible safety hazards? Anything that just does not look right?

JDLR (Just doesn't look right)—I don't know who coined this phrase, but it fits here perfectly. As your officer is video patrolling, she or he may see something that JDLR. This is where the camera has the advantage: keep watching the activity until it looks right. Otherwise, it may be something that requires personal attention.

Once a suspicious or important activity is identified that will require video coverage, such as a fight or theft in progress, the surveillance officer will manually place cameras. First is the suspect shot. The camera that has been following the suspect should remain on the suspect to get facial images and detail of the actual crime. Second is an overview shot. This angle shows the suspect in relation to his location (e.g., overview of the store, the lobby, or the dance floor). Third is also an overview, but at a slightly closer and opposing angle. This view will show the suspect's and accomplice's faces, hands, and contact with responding officers.

We discussed the need and use for cameras and alarm systems in several other locations in this book. Cameras, if watched live, can add more sets of eyes to the behavioral recognition process. Panic alarms can provide notification as described previously. In a large hotel with a security force and a video monitoring room, the advantage is obvious. A smaller hotel that may have a front desk associate and a night auditor also can make use of these types of alarms as signaling devices. When a suspicious person enters the building, the first employee could activate a button that simply notifies the other employee in the back that something is happening. Similarly, in a small operation, a door entry alert will let everyone know that someone has walked in so that he or she can be monitored.

Camera Placement

I had a GM tell me once that the US Park Service does not install walking trails in National Parks until they have been open a while. His point was, do not try to anticipate the need for cameras at certain areas. Let the guests decide where cameras are needed based on their actions.

Chances are you already know the answers to the above query. I urge you not to put all your cameras in one basket. Cameras are inexpensive now and so is data storage, so the temptation is to put the darned things everywhere. There is a problem with that. Who is going to watch 400 cameras? Or 1,000? Put some thought and strategy into this and use them where you need them.

One night, a group of teenagers came inside the property. Everything was closed but they were looking for some fun or mischief or both. They used the restroom and when they came out, they got into an argument with a middle-aged couple of hotel guests. One of the teens went to his car, retrieved a firearm and came back and shot one of the guests in the neck.

Fortunately, we had facial cameras located at each restroom. We were able to not only get a nice facial picture of each suspect, but we also caught most of the shooting from the same camera.

Whenever I install a camera, I make sure I am at least getting double duty from it. For example, if you install a camera to watch a door, try mounting at the door facing out. You don't need a picture of a door—you can catch the face of anyone approaching the door as well as whatever is in the background.

Let's agree first on the purpose of cameras. Guest safety. That is always your first answer. The temptation may be to say we have a problem with kids stealing gumballs out of the machine in the lobby and put a couple cameras there. No no no. Think about it. $1,000 to save $2.00? No no no. What is worth with this waste of resources is that the time you spend watching a camera to catch the bubble gum bandits, you could have spent watching real criminals threatening your guests. But seriously, how do cameras keep guests safe? ONLY IF SOMEONE IS MONITORING THEM IN REAL TIME. If a camera is not live-monitored, it only has investigative value, which is too late for safety, but is still useful as I will explain later.

Suppose you have a scary sidewalk outside that is a bit dark and secluded. You put a camera there to protect guests. First, I will tell you that robbers do not case the joint. They do not even look up. They are focused on their next fix (of drugs) and are too short-sighted to think a crime through to its prosecution. They will get in, get out, and care less if there is a camera there. Second, a well-placed camera means that someone must be able to see the crime occurring and call the police, send security, or run out there personally to save the guest. We all know that does not work.

A better solution is to protect that scary sidewalk and reduce the risks there. Install lighting, change landscape to make it more visible from the parking lot, and most of all, eliminate it. Make a more welcoming path for your guests instead of trying to catch the ones who prey on them. Cameras do much better when they are in a location where they can prevent problems. A camera located outside, that views the porte cochère, will alert you to a suspicious person before he walks in the door. This gives you time to take some other preventive action. In a small to medium-sized hotel, I recommend cameras be deployed in the following manner.

Cameras should be in any area a guest can go that is not visible to others 100%. This would include the pool, laundry, back hallways, everywhere outside. These primary cameras should be monitored. (If someone walks into your pool area that is unoccupied, you want to know that immediately.) There are ways to set cameras to alert you to motion or other triggers of activity.

Other cameras are used for live investigation, such as watching that suspicious person walk through your property. Therefore, camera should be placed at every chokepoint and every intersection of thoroughfares. It is not necessary to have eyes on the person every foot of their journey. A long hall for instance with no other outlets, just needs cameras at each end. You do not need to see the person walk down a hall.

Finally, yes, we do need cameras for post-incident investigation, to sum up. If you have the ability to cover your entire facility, go for it. As long as there is no expectation to watch those images live, it will be nice to have full coverage to investigate incidents. If you are "camera poor," make sure entries and exits are covered.

Some other camera tips. Mount as many cameras at eye level as you can. With hoodies and other obstacles, it is difficult to get a facial shot from a ceiling camera. Cameras are easily installed in door frames or right on a wall. I had cameras mounted at restroom entrances. Everyone visits the restroom, and you get a nice portrait of them as they go in to do their business.

If you have revenue centers such as bars and retail, you need a camera directly over the register to see money and transactions, another over the sales area to see the merchandise and the transaction. The third camera is an overview that can see the faces and placement of involved persons.

A great camera for the front desk is mounted on the counter, perhaps right near the credit card machine. If someone is shy, by the time they see it, their image is already captured. This is useful for fraudulent check investigations.

Cameras can be mounted in your ATMs—well just about anywhere. Remember some ethics with cameras. You do not want to see PIN numbers or into a dressing room. Even closets and storerooms would be off my list.

Use your cameras in conjunction with other resources to reduce pilferage. For example, if you are having liquor bottles go missing from the storeroom, you do not necessarily need a camera in the storeroom. Using your inventory data, narrow down the time the bottle was taken, then use the facial camera just outside the storeroom to capture your suspect. Remember from the investigations chapter that you do not need to witness a crime to terminate an employee. All you need is a policy violation.

I also recommend cameras on each end of an escalator to capture accidents. Cameras in elevators are invaluable for investigations in your hotel—definitely at the elevator bank.

Hotel hallway cameras are a bit controversial. If a hotel is not wired for cameras, it is expensive to add them. Then there is the dilemma of watching them live or just for investigations. They do not have great value in investigations, frankly, but certainly is nice to have them. You can use a lock interrogation and the elevator cameras to get the same story. Most major chain properties would like to have cameras in hallways, but if they install them in one, they would have to install them in all. So I doubt you will be installing them up there also.

More on cameras and video in Chapter 12.

SPECIAL TRAINING

Bike Patrol

Bicycles have been used for patrol for over 100 years, but organized training and policies did not really become part of the program until the late 1980s. Many police departments claim to have originated the official training style that has permeated security and police departments all over the world. My first experience was in 1993 with two Seattle police officers who developed a training program for police that included safety, coordination, riding techniques, and equipment selection. The training program I developed evolved from that one after I modified it for the armed security officer.

Today, Bike Officers are common in all sorts of outdoor patrol areas, especially parking lots and structures. With all the technology available today, I still believe that bike patrol is the most effective layer of security in a parking area. Combined with cameras, gates, signs and all the other layers we all use, bikes can be effective in prevention. In fact, you may have noticed in the past 30 years that when police have gotten out of their cars and onto bikes, they too became more effective. They went immediately from response to prevention and from introverted car drivers to outgoing PR magnets. Unfortunately, they are still viewed as an extra or a luxury for police as they cannot afford to replace a beat car that covers several square miles with a bike that covers a few square blocks. Security, however, can save money with bikes. If not a money-saving, you surely get more value with a bike because they cover more area faster than a walking officer.

Bikes are visible and stealthy at the same time. Customers will easily approach a bike to ask directions or even talk about bikes. Kids will approach a bike officer to ask about his gun or his handlebars or whatever. Adults are often intrigued. I noticed a mark drop in outside crime and complaints after we initiated a bike patrol. It was rumored that the bad guys on the street were warning others to stay away from that place. They have bikes!!

Thirty years later, many manufacturers sell mountain bikes designed for urban patrol. The primary difference between these and a regular mountain bike is their durability. Weight is sacrificed for strength in the frame and components. Since patrol bikes will be ridden almost entirely on concrete as opposed to dirt, this durability absolutely prohibits buying a bike off the rack at a bike shop. Just as a police car is modified for constant use and abuse, so should a patrol bike be built for bumps, jumps, and maybe even a heavier rider. Rather than custom building a bike, find a manufacturer that makes "police" bikes.

Helmets and gloves are basic, but apparel must have the attributes of a security uniform and the comfort and flexibility of bike shorts and shirts. Lighting, reflectors, and other safety equipment are standard.

A qualified mechanic and a bike shop should make repairs. You can try to create your own shop, but by the time you count labor and the cost of inventory and special tools, it is faster and cheaper to have repairs done by a professional.

A certified bike patrol instructor should train bike officers. Many renowned organizations certify training, and they offer classes for instructors. Some hotels rely on their local police departments for this training. Ensure that the training includes the following components:

Bike patrol policies—These include use of force with the bicycle. The bicycle can uniquely fit each of the levels in a use of force policy from presence to deadly force. Other policies include where it can be ridden, pursuit policies, and sidewalk or road-riding laws.
Repair procedures—Training should include basics like minor adjustments, flat repairs, and safety inspections.
Control and coordination—Bike officers need to be shown how to control the bike at slow speeds, ride through crowds, use pedal straps, ride with one hand, etc.
Riding techniques—Speed-shifting, emergency braking, obstacle avoidance, curb and stair climbs and descents, and even falling are important parts of the overall training.
Dismounts—Patrol officers learn to use the bike as a tool and even a weapon for apprehending criminals.

Training for bike officers should be at least three days and include long-distance and strenuous rides to evaluate endurance and stamina of the riders. Other specialized patrol functions are discussed in Chapter 3.

Escalators

If you do not have escalators in your facility, you are fortunate. Escalators seem to me like big shredders or prehistoric raptors that knock people down and eat them. I am waiting for someone to invent one that is not made of sharp teeth. The sharp teeth inflict most of the injuries, but it is generally the person wanting to go up or down that is to blame for their fall.

I also find it unusual that people traverse escalators in airports and subways all the time without a problem. The hotel is a different story. I have watched this for 30 years and those that fall are:

- Elderly who have trouble with their gait, neuropathy, propensity to fall, etc.
- Persons who have genuinely never used the steel shredding beast. Yes, I have seen youngsters coaxing their mother to step on and the mother trying to time her first step.
- Kids engaging in horseplay
- Persons trying to control their luggage.
- Persons in scooters or wheelchairs. Yes, I have seen people drive right on in their chair as if it will pick them up like a conveyor and take them right up.
- Persons with rubber shoes (named after a reptile), sandals, barefoot, slippers, untied laces, etc. Escalators eat these delightful treats. Occasionally they pull the toes into the teeth (combs) as well.
- Dogs tend to leave their shoes home when on vacation, so keep them off the escalator. It will eat dog toes as easily as sandals and shoelaces. Ouch.
- Once the loss of footing occurs, there is little to be done. Going down, the rider is likely to tumble several steps down. Going up, gravity takes over and pulls the person down toward the bottom. Falling down steel stairs is bad enough, but those sharp edges mutilate the skin horribly.

The escalator has safety switches that detect jerking and other strange notions and may stop. But the faster someone gets to the stop button, the better. I spend some pages on this topic so that you can train your staff (not just security) to stop the escalator first and ask questions later.

Response to an escalator injury is explained in Chapter 7.

There are some other risks associated with escalators. Let me give you my layperson's explanation of the mechanics so you will know what I am talking about. There is a substantially large electric motor that drives a heavy chain all the way to the top (like a motorcycle); the chain holds each step which has wheels that glide on rails. The handrail is like a fan belt—a long ring of rubber that is also driven by the motor. Like an elevator, there are safety brakes that are open when operating, but clamp down hard when the stairs stop. The brakes are generally installed on the motor or the pulley that drives the chain. The brakes are the weakest link and can fail if overloaded. When an escalator is stopped for whatever reason, the brakes are keeping the stairs from sliding down the rails out of control.

Whenever someone climbs or descends a stopped escalator, they are putting weight on those brakes. The brakes can handle this normally, but after years of this abuse, can fail, causing the escalator to "fall." I have seen videos where the escalator is overloaded, and it collapses and tumbles everyone down to the bottom like toys (check these videos online). For this reason, you should make sure guests do not use escalators that are not moving.

Another calamity that is more common derives from a very busy escalator that has a person on every step. Everything is going along just fine until the persons reaching the landing stop (to look around or because there is a traffic jam in front of them). Again, the tin soldiers go tumbling as they are carried into the dogpile with nowhere else to go. I recommend monitoring escalators when they are extremely busy such as for a convention.

Elevators are not as injurious as their diagonal cousins, but still require some knowledgeable response and prevention. Elevators are either lifted up and down from the top with a motor and cables or pushed up and down with a hydraulic piston (like at the tire shop). The hydraulics are generally shorter in height because of the limitations of the piston. For safety, the elevator "car" has brakes, which like the escalator are open when it is traveling normally, but clamps down to stop the elevator when power is lost or when it detects a free fall or other problem. It is rare to have a modern elevator fall out of control because of many safety devices. Here are some incidents that I have seen.

Elevator becomes stuck. This is usually a computer problem, or a safety switch has activated those brakes. The most common reason I have seen is kids jumping up and down in the car. This makes the car think it has lost control and stops. Power failures can also stop an escalator. These problems are usually resolved with a re-boot of the elevator (by a qualified technician). This is where another problem can occur.

In rare instances, it will be necessary to manually open the doors to extract the occupants. This should be done by the fire department or the elevator mechanic ONLY. You do not want the elevator to be reset while you have people climbing out the door. Ouch.

It is difficult for elevator riders to open the doors, but exasperation makes people very resourceful. An inner elevator door that is open can expose the guest to moving parts that are not supposed to be exposed. I have seen people open the inner and outer doors and climb three feet to the floor level, risking the guillotine effect. When a technician opens those doors, he/she will first go to the machine room and lock it out so that it cannot move. Think about a miscommunication between him and the fire department or between your maintenance person and the technician.

Elevators that are stuck (we always called it "delayed" so that other guests would not hear that we had guests trapped. The fire department calls it an entrapment, as a matter of fact) with at-risk humans on board, creates a secondary problem. Claustrophobia, pregnancy, and mental instability can cause panic and physical problems that will leave them helpless.

On one sole occasion, I saw a woman lose the tip of her finger in the doors. We all lunge our hand between the doors to catch a closing elevator. The safety switches that open the doors may be far enough apart to miss the finger and close tightly on it.

Overcrowding, which tends to cause the delay in the first place, makes for an uncomfortable time in a delayed elevator.

Before you operate elevators, make sure you have an arrangement with the elevator company or someone that can respond quickly when you have an entrapment. If not, you will have to call the fire department, and they bring those steel pike poles with them. In fact, sometimes the occupants will call 911 and then the friendly flame tamers will show up with those same tools. If they feel access to the car is urgent and you cannot assure them it will be fixed soon, they will open it with the heavy equipment.

Another preparation you can do is make sure the communication device inside the elevator is operable (two-way) and is answered 24/7. Have someone that can stay on the phone with them and keep them calm until help arrives.

Cameras in elevators are useful for entrapments. They are discussed in chapter 12. Use them or ask for them if you do not have them.

Spas and Pools

Spas and pools usually occupy the same space and are probably managed by the same person but have some different security issues. Pools (for recreational swimming) are a huge liability and need some specific measures to prevent safety concerns. Spas (where special treatments are provided) are more like a retail outlet and have those same security concerns.

Lifeguards

It is important to discuss the needs for having a lifeguard with your property risk manager. Many properties have gotten away from this service and chosen the “swim at your own risk” philosophy. This is partially due to cost and partly because lifeguards take on the entire burden of safety. If something happens, it will be the fault of the company whether it was or not. Other properties have taken the middle road and provide a towel attendant whose job is to control access to the pool without really taking responsibility for people swimming. Some properties still provide full-time lifeguards. These personnel must be trained and supervised and can protect the facility from the guests while protecting the guests from the water. The decision of which water safety posture, probably not made by you, will take several things into account: size and depth of the pool, type of clientele (families, children, elderly), and other safety measures in place (cameras, lifesaving equipment, gates, windows, etc.).

If you are going to have a lifeguard, this is going to be the most important person on your staff. Her training cannot be compromised, and her performance must be 100%. Falling asleep, failure to act, and inattention to duty can lead to a tragic death, which could close a pool and maybe a hotel. Whatever certifications are in place for lifeguards in your jurisdiction, exceed them. Scheduling must be absolute. Will you have a hotel security officer cover breaks? What about his training? The lifeguard will have to enforce pool rules, have the proper equipment, and know his job and the security function very well.

Pool Rules

Most pool rules are standard and can be purchased on ready-made signs. These include no running, no diving, no urinating, etc. There may be other rules that are specific to your hotel. Depending on your lifeguard presence, you may want to prohibit unattended minors, alcohol, food, and toys. Make sure the rules are clearly posted and enforced. Remember that signs are not an enforcement tool, but a warning mechanism.

Safety Equipment

Make sure the basics are present and supplement wherever you can. The cost of safety equipment pales in comparison to a death. Recovery poles, life preservers, depth indicators, and CPR instruction signage are easily provided tools. Check with your local parks department and other public pools for ideas and standards. An emergency phone, panic button, or other instant alert device is advisable whether the pool is staffed or not.

> In 2002, the first publicized death from a pool drain suction occurred at a resort swimming pool. This phenomenon, which was completely unknown to most pool operators, took the lives of several adults and children before federal legislation was enacted to prevent the deaths through awareness and physical modifications. The danger occurs when someone would get caught in the suction from the main drain (in the bottom of the pool). The suction was so intense it would either hold the victim down and drown them or eviscerate (disembowel) them. The preventive measure was to either install an anti-suction valve or to cover the drain so that no seal could be made to the body. This fluke of a hazard highlights the need to have someone present when anyone is swimming.

Hot Tubs

Hot tubs, Jacuzzis, whirlpools, whirling jet tubs—whatever you want to call it, these relaxing and therapeutic little pools are associated with many types of deaths and injuries. Besides the effect of the hot water on the bloodstream, there have been several bizarre deaths caused by hair getting caught in drain covers, the suction of the drain described in the textbox. A rare bacteria disease from the steam has caused enough deaths to warrant a good safety plan for your hot tub. Temperature monitoring and automatic cutoffs are vital to keeping the water temperature at a safe level. Manual emergency stops are also a necessity. Alcohol use in a hot tub increases drowsiness and decreases judgment. Sexual assault is another matter not related to your equipment and maintenance. Make sure the security plan for your hot tub does not overlook these threats.

Spa Treatments

If your hotel has an actual spa, then you probably provide massages and various other relaxation and cosmetic services. Unlike the other components of your spa, which are equipment-related, these amenities are service-based. Therefore, the risks associated with services are similar to those found in the Retail and Restaurant departments. Check those sections in this chapter for concerns that cross over into all revenue-generating departments: retail theft, fraud, etc.

There are also some risks uniquely associated with spas that need to be considered by Security. These include, but are not limited to, sexual assault and abuse, loss of stored guest property, health reactions to treatments, and sanitary health issues. These are not deal-breakers, but should be addressed in advance by legal counsel, Security, and spa management. Some simple rules that are enforced by Security can prevent most of these incidents.

Chemical Hazards

Sometimes we forget that pool chemicals are some of the most toxic substances in existence. Chlorine (sodium hypochlorite, or similar) used to sanitize pools is deadly if inhaled or ingested. Hydrochloric acid is used to balance the pH in the water. Large pools may have tanks with automatic dispensers. These should be perfectly safe, but are susceptible to earthquakes, tornadoes, and hurricanes, as well as terrorism and tampering. Make sure pool chemicals are secured in an OSHA-approved and fire-rated container or cabinet that is locked and away from guests.

In 2010, a major hotel was having its outdoor pool system repaired by an outside contractor. The valve controlling release of the chemicals was accidentally left on, so the pool was flooded with too much of the toxic substance. The chlorine was diluted enough to be less than lethal, but as it evaporated, the gas was inhaled by 100 of the 1,500 pool users. Twenty-six of those persons went to the hospital, the pool and surrounding area was closed, and the hotel paid out money to settle dozens of claims as well as being fined by OSHA. The hotel sued the contractor and settled with the contractor. Although the hotel was not entirely at fault, it definitely suffered losses.

Pool Parties (Wet Clubs)

Pool parties have become big business in many larger hotels in cities throughout the world. These are not the pool parties you have at home for your child’s tenth birthday but are a successful way to convert an existing amenity into a lively venue at night. Many of the risks and concerns associated with pool parties also are present in nightclubs, so go to Nightclubs chapter and review it with your pool in mind.

Combining the risks of having a pool and the risks of having a nightclub will not cover the new and unique risks associated with pool parties. After all, during the day you probably do not allow alcohol or even glassware anywhere near your pool, but at pool parties they will be prevalent. Your security presence will drastically change. The pool may or may not be covered or open for swimming. Your beverage department will install new fixtures, cabanas, seating, electronic equipment, lights, and music. Make sure you do a thorough, and separate, Risk Assessment and Security Plan for pool parties. The plan for a family swimming pool is different from the one for pool parties. You will need new post orders as well.

Theft

Theft from lockers and of items left around the pool is common. As in other parts of the hotel, patrol will help prevent these crimes. Officers should make sure lockers are secured and that items are not left unattended. Limiting pool access to hotel guests with keys helps but does not eliminate theft. Hotel guests steal from each other, too. Signage is a common way to mitigate loss. Usually, the signage will focus on how the hotel is not responsible for theft or damage. Go the extra step and offer tips on how to prevent it. ("Please do not leave valuables unattended. Lockers are provided for your security and convenience.")

Valet

Your legal department has no doubt written a disclaimer that is printed on the back of every Valet claim ticket. "This contract limits our liability …" does not necessarily limit your responsibility to take reasonable care of the guest's property. This means you and your Valet department need to take reasonable precautions to secure guests' keys, vehicles, and their contents. Like everywhere else, there needs to be controls in place for these safeguards.

Keys should never be left in vehicles. Establish a procedure where the attendant receives the car from the guest, completes the ticket, and secures the car and the keys. It is common for a thief to walk through Valet looking for the keys in cars and drive off, or worse to impersonate a valet attendant and take a car from a guest.

The valet office or key box needs to be secured every second. Combination lock keypads are popular, but easily thwarted by anyone watching. Valet attendants are in a hurry to take care of their guests, so they tend to bypass locks and procedures that slow them down. Locked doors tend to get propped open. Keys in vehicles find themselves out of sight, but within reach—visor, floor mat, etc. Look into a card swipe or something similar that will allow fast access but keep our guests' property secure. Think of the value of all those keys and your hotel's reputation if you lose them.

The parking area should be as secure as possible. Fencing, lighting, controlled access, and patrol are very important here. Make sure attendants are securing vehicles by having security officers check doors and windows on a regular basis. I bet if you patrol your valet parking area, you will find at least one vehicle unlocked every day. Better you than a burglar.

Your parking area should have speed limits posted and Valet employees need to follow it. Security can help monitor this, but good supervision should catch offenders. Reckless drivers should be dealt with swiftly and sternly. Avoid putting time constraints on Valet drivers. They have enough incentive to hustle—tips.

Remember the pizza company that promised delivery in 30 minutes or it's free? That marketing campaign was ended in 1993 after several multi-million-dollar lawsuits claimed that pizza delivery drivers were driving recklessly to meet the goal. The pizza company did not agree that the ads were the cause of several serious injury accidents but pulled the slogan anyway. What does this have to do with Valet? Tell your employees to hurry when returning cars and they likely will, even if it puts property at risk.

Employee Theft

Internal theft is a temptation for Valet employees. Guests will make claims alleging theft, damage, and abuse of their vehicles, and more often than not, it is a false claim. All these claims need to be investigated. Valet is a difficult area to prevent internal crime because of the mobility of the attendants. Just like Housekeeping, it is unusual for a Valet attendant to engage in minor theft from a vehicle. It does not make sense for them to risk their job for the change in an ashtray or some CDs. If you do have an attendant stealing, you will know it because of the pattern of thefts in that area. See Chapter 8 for more information on investigating internal theft. Random patrol and some camera coverage will prevent most of what the previously mentioned controls will not.

Guest Accidents and Injuries

Combining moving vehicles with pedestrians is likely to result in accidents. You have a responsibility to prevent accidents as best you can. Having guests walk across the concourse should be avoided, but if it cannot, you will need to take some extra steps. The minimum might be a painted crosswalk and speed bumps. At most, you might consider a “crossing guard.” This could be a security officer, bell person, doorman, or taxi attendant. Remember that guests coming in are tired and anxious for relaxation and guests going out are preoccupied with their drive and all of their belongings. Either way, they are not as cautious as a regular pedestrian, so take extra care in protecting your guests.

Vehicle Damage

It is common for guests to claim damage to their vehicle after retrieving it from Valet. Like theft, it is not likely that a Valet attendant will damage a vehicle while it is in his possession. There are some measures you should implement, or at least consider, for your Valet. First, make sure attendants inspect the car before taking possession of it from the guest. Once they get good at it, this will be a fast and simple habit. Note damage on the rear of the ticket. Second, encourage employees to admit when they damage a car. Terminate them if they do not. Third, some hotels install camera systems that inspect the vehicle as it leaves the Valet concourse. These are nice if you can justify the expense. If you are having so many damage claims to make this a worthwhile investment, you might consider some other options like driver training, hiring experienced drivers, reconfiguring the parking area and route, and discipline for damage.

CONVENTIONS, MEETINGS, AND BANQUETS

Convention centers in most hotels consist of meeting and exhibition space and kitchen. These areas need to be patrolled after hours to make sure they are secure and employees or guests are not intruding into closed areas. During hours of use, Security will depend on what clientele are being catered to in those spaces.

Most hotels have meeting space to supplement their room inventory. Meetings, banquets, conventions, receptions all fit in with the hotel nicely. Banquets allow for the food and beverage department to enhance its revenue, especially if there is already a restaurant. Meetings provide for more sales of rooms, especially for businesses that travel on the weekends. So, weddings, parties, Quinceañeras, and real estate symposiums on the weekends; and meetings, awards ceremonies, trade shows and expos on the weekdays. The hotel loves this side business, and it can make or break a large or small hotel.

Large hotels may use their meeting space for larger assemblies like concerts, comedy shows, and conventions. Where there are people, there is risk, so there is security. Here is where you come in.

Your in-house meeting staff is usually a bit naïve about the need for security, especially for a gathering of businesspersons for a few hours. What could happen? They are correct, in most cases, but like everything else, it is the exception that gets people into trouble. The only way we must prove that our security plan is effective, is to show negative data—or stuff that did not happen. That is difficult to do. Another solution is to recommend a security presence at every meeting. I offer a process and some policies that can guide everyone through a safe and secure meeting, banquet, or party.

Security needs a seat at the table for event planning. Whether it is a rehearsal dinner for a small wedding or a statewide political convention, there will be risks and threats. If those are not met, then you have negligence and safety problems. Your catering and sales teams already have planning meetings to prepare for these events. You just need to get invited. In the beginning, I would use these meetings, not only for their practical value, but also to educate yourself and the catering folks as to security policies and their reasons.

Trying to institute security measures once an event has been planned and paid is exceedingly difficult. It is best to offer up security policies and challenges to the group in the concept phase when concessions can be made, and some negotiating can take place. So instead of going in with these decisions already made, approach the group with your objectives—which should be the same—and work on solutions together that are effective and within budget. Of all the things to be concerned about at any event, I think you can limit yourself to two: Alcohol Consumption and Crowds. The color of the napkins and choice of music can be left to those professionals.

Each event should have a risk assessment and security plan. I am not talking about a 100-page document, but even your notes from the meeting may suffice. I am also not saying that every event will have security. A ten-person board meeting will not, unless it involves some special circumstances.

Years ago, one of my hotels hosted a restaurant food association. One of the topics was goose liver. I had no idea that goose liver was such a controversial food until we started getting threats. I had a quick education on how goose liver is used in restaurants and the controversy it caused, due to the way it was harvested. Apparently, there are animal rights groups that oppose the harvesting of the goose liver. We figured out the day of the event that there would be protesters showing up at the event and making a big deal. I had no idea.

Now you must assess and then plan for the event. As always, I start with the objectives. The objectives will be your question list for going to the meeting. Rather than list your questions/objectives here, I will jump to the concerns you would have at an event.

Event Type

You need to find the type of group—Party, Expo, Meeting(s), wedding, concert, etc. Most of the risks are obvious and the others, you get from me or your colleagues who have hosted similar events. A few professional education tracks versus a teenage rap party are extreme examples. The professional group has hardly any risks (above normal) and the teenagers have the potential for violence, horseplay, drinking, and sex.

Specific Group

Get the name of the group (band, show, expo, etc.). If you are not familiar, look them up. If you are unsure of the risks involved, call your equal at the last facility they used. Check news reports, even the police if you think it is necessary. Blindly planning for an event without knowing its history would be negligent, in my opinion.

Number of People and Demographics

The number of people involved is going to determine things like fire exits. The other demographics will allow you to take age and other factors into consideration. The International Fire Code requires Crowd Managers now for assemblies of 250 persons or more. There has to be one certified crowd manager for every 250 persons. Crowd Managers can be from any department as long as they have the training. Online training can be found by searching "crowd manager training." Your local fire department may teach it or have a local vendor. This is one area where Security can have dual roles: Security and Crowd Manager.

Alcohol

If it were not for alcohol provision at many events, we would not need to be there. Alcohol can make a somber event a bit rowdier as you know. It also puts the hotel at risk if something happens as a result of someone being served—or over-served. To determine whether you need a security presence, will have to depend on what you know and what your event staff tells you. A dinner party of ten persons may not need an officer as long as you have a responsible bartender with a supervisor checking in on them. Large events will have to have security to assist the bartender with serving protocol. Intoxicated guests will have more accidents, arguments, and horseplay than sober ones.

BYOB

"Bring Your Own Beer." When your guests see your liquor prices, they will be angry. They fail to realize that since we do not charge for the room and the staff and the tables and chairs and all the other amenities, we have a lot of overhead. It also helps us slow the intake a little. You will still have resentful clients and attendees who will smuggle their own alcohol. This needs to be prohibited and even grounds for ejection. Not only is it (probably) against the law in your jurisdiction, it prevents us from monitoring alcohol intake, thus jeopardizing our license and everyone's safety.

Music

Music adds a bit more risk because it is loud, gets everyone animated, and increases endorphins. Without pretending to be a doctor, I can tell you that people who are moving around (dancing, exercising) are more likely to get physical. I would treat parties, concerts, exhibitions (with alcohol) like a nightclub and staff it accordingly. See Chapter 10.

Politics

Unfortunately, we are divided into many ideologies and groups based on politics, activism, education—almost anything. Like my goose example above, it may not be the event, but those who would oppose it. Research and intelligence from local authorities will help—and they will likely appreciate the heads-up anyway.

If you have a convention center, or multiple rooms where you can schedule more than one event at a time, find out what events are running concurrently. You do not want conflicting groups together.

Admission

Who is monitoring authorized attendees? Tickets? Admission? Age? Your event staff may want to delegate some tasks to Security. No. We do not want our people distracted by another job when alcohol consumption is so critical.

Merchandise

Will you be responsible for securing and guarding merchandise? This is more hours and more bodies you must provide. Depending on the merchandise involved, it may mean even more. Jewelry show? Gun Show? What about raffle prizes? What about a raffle prize that is a GUN? (Hey, I am from the Wild West.)

Security

Don't tell me they are bringing their own security! This never works out well and it has the potential for being really bad. Choose your own people, even if you have to contract it. If you do contract, get the policies, rules, appearance, and rules of engagement set prior to the event. They must have Alcohol Awareness Training if alcohol is at your event.

Dress and Prohibited Items

For some events you may want a dress code just to make sure you do not attract the wrong crowd. This would only matter for events open to public. You should have a policy that is enforced consistently with every event that prohibits weapons, dangerous materials, and so forth. The Food and Beverage Chapter has some guidance on dress codes and prohibited items.

Age

A big "threat" to any event with alcohol is serving minors. Find out who is checking ages of attendees, if they are segregated, etc. Who will check IDs? Do not leave that up to the client.

Crowd Management

I mentioned this earlier regarding overcrowding and evacuations, but you also need to plan for queue lines, check points—if any—exit routes, etc. I worked a hotel that had a multipurpose hall that seated 1,500 for assemblies. This room was in the basement, accessed by escalators. At the culmination of the concerts, we had to post escalator monitors to prevent overloading and pileups on the escalators. Crowd Management is discussed in more detail in Chapter 11.

Minor Events

A quinceañera, which is what Americans might call a "debutante" ball, is a traditional rite of passage for 15-year-old Hispanic girls. The parents will spend more on this party than their daughter's wedding. Unlike a wedding, these gatherings are more difficult to manage. The Latin culture is familial, and close friends are considered cousins and uncles, while the relationship with blood relatives is sometimes contentious. This means a guest list that is already provoking violence before the event is publicized. Publicity is another problem for you. Hispanics generally do not use guest lists, invitations, and RSVPs for gatherings in most cases. Everyone is welcome and "we will make the food last all night." This does not work for a hotel that charges per plate or per seat. Quinceañeras can be lucrative and safe if security is involved and takes precautions. (This goes for other young adult events like fraternity parties.) This requires a guest list or invitations only. Client is paying per person and we cannot manage an event that has open doors. Use a checkpoint to ensure no weapons or alcohol gets in.

Like everything else we do, we need to plan for every foreseeable circumstance, or we will fail. Assess the risk, plan for mitigation, keep safety above revenue.

Security Plan

Just like the hotel Security Plan, the individual Risk Assessment will determine the security deployment for each event. You may be able to set up standard staffing levels for some event types so your convention managers can work this out with the client in advance. For example, rap concerts and teenage birthday parties may require guest searches and bag checks at the door. Exhibitions may require an officer at each entrance and exit. You can also establish staffing proportions such as 1 officer for every 100 attendees. (Search stations are discussed in this chapter under Security Measures.)

It is a good idea to require the same security posture for each type of event. Avoid allegations of discrimination if you require searches for black rap groups and not for white country bands.

Special Event Permits

Your Convention Manager will generally take care of special permits for certain events and these vary by jurisdiction. Your involvement may be required for the fire inspection, if there is one. The event space has already passed code inspections, so if everything is kept the same, there is little to worry about for a special inspection. However, some events will want to block certain exits, extend above acceptable clearance levels, exceed occupancy levels, etc. There may be requirements for flame retardant wall coverings, vehicles being parked in an occupied space, and so forth. This can be a complicated set of rules, so it is best to establish a relationship with your local fire inspector so you know your expectations in advance. Allow enough time to make changes to layouts between the inspection and the event.

Outdoor Events

Expanding our available resources by hosting events outdoors is a testament to the flexibility and creativity of your sales and catering staff. Support these events as we discussed in the last chapter but be aware of some special considerations.

Weather is a threat as we talked about in Chapter 1. If you have an outdoor event, make sure you are aware of seasonal weather patterns for your area as well as monitoring weather systems as the event gets closer. Work out an arrangement with your event planner as to who will have the authority and ability to cancel or change the event at the last minute if weather dictates. Make sure your temporary structures (tents, stages, lighting, signs, etc.) are constructed with weather (wind, mostly) in mind.

> At the Indiana State fair in 2011, an outdoor stage took a 60-mph wind gust and blew over. Five people were killed by the gust, which was unforeseen and described as a “fluke.” The organizers had been in contact with the National Weather Service, but there was no indication of heavy winds.
>
> When we build permanent structures, we plan for every possible type of weather or disaster. Temporary structures are generally not suited to withstand extreme weather. Make sure your Risk Assessment and incident action plan for your outdoor event considers these extreme events.

Access control is another issue that is more difficult outside. You do not have your normal walls, gates, cameras, and other "levels" in place. Your security plan for the event should tell you whether you might want to install temporary cameras, gates, turnstiles, etc. These are more common than you think, and just about anything can be rented these days.

Remember staffing for outdoor events. Do not expect to "cover" an outdoor event with existing staff. This is going to leave another area weak. Use overtime or hire an outside source to make sure you have adequate personnel to protect your assets and counter threats.

PARKING

Parking is a huge responsibility that is generally given to the Security Department. Besides being responsible for protecting the assets of the lot or garage, you may be responsible for other aspects of parking as well. Here are some of them.

Cleanliness

You know that garage downtown? You know the one: Graffiti on the back alley side, signs hanging crooked, sidewalk all beaten up and lights out on every floor. The pavement is so oily and dirty, you cannot see the original gray concrete color. And forget about the walls. They have so much brake dust and soot on them that the lights do not stand a chance at keeping the garage properly lighted. I hope this does not sound like your garage. This type of place scares away the bravest among us. Imagine how employees and guests would feel. It is no longer just a theory that dirty, dark, unkempt places promote more crime and violence.

An area that appears well kept, clean, and often traveled is less likely to experience crime. We have all seen how an abandoned building maintains its appearance until that first window is broken or wall is vandalized with spray paint. The same is true for parking lots. Keep your garage or parking lot free from trash, road sand, and debris. Ask your environmental services crew to assign someone to this area full time to pick up, sweep, and empty trashcans. Guests who stop at your hotel on a long road trip will use your garage to dump their trash and empty coolers. Have sufficient trash receptacles for this purpose and keep an eye out for trash dumps throughout the parking area.

Graffiti should be reported and expunged immediately. One tag is all it takes for graffiti to multiply. This makes guests feel uncomfortable anyway. In an established gang area, a tag may indicate "ownership" of turf and send the green light to local car burglars and vandals that your lot is wide open. I always kept a can of graffiti remover in my desk drawer because the sooner you get it off, the less likely more tagging will occur. Garages and bathrooms should be as clean as the rest of the building—and more so.

Abandoned vehicles should be addressed before they become obvious to others. Keep a long-term parking log for guests and employees who leave their cars parked while they take vacations or look for a spare tire. You can mark cars that are parked over two weeks and then tow them after another week.

In 1982, James Wilson and George Kelling wrote the Broken Windows Theory. This theory asserts that one broken window in an abandoned building soon attracts more vandalism and ultimately squatters, arson, and blight. The theory also applies to abandoned cars in parking lots and litter on sidewalks. New York Mayor Rudy Giuliani made the theory famous and proved it right when he applied the theory to the New York subway system. Targeting minor crimes and visible nuisances lowered the major crime rate for 10 years in that city.

This theory can be applied to your parking garage. Abandoned cars, litter, graffiti, and other minor vandalism, if immediately resolved, will keep other crimes at a minimum.

Lighting

There are minimum industry lighting standards for parking lots and garages. I suggest you exceed those until your garage or lot feels safe and comfortable. Your facilities manager will want to use cost-efficient light bulbs that turn the garage yellow or fluorescent white. Get involved in this process and make sure it stays bright and pleasant. Trash sweepers and Security personnel should be aware of lights that are out and get them replaced immediately. This goes back to the Broken Windows Theory.

Cleanliness, that we just discussed, affects lighting. Lights need white walls from which to bounce light. Get a spray washer if you do not have one and ask someone to clean from the top down and when they get to the bottom, to start over again. It is worth it.

Access Control

Even if you have free parking, access control to your parking area allows you to limit and track parking usage. It also allows you “the greeter” effect for potential troublemakers. If the garage has free ingress and egress, a burglar will feel much more comfortable entering to case cars. If he has to stop and take a ticket or be greeted by an employee, he is less likely to chance being remembered.

License plate recognition has become advanced, yet inexpensive, and can be a great security and marketing tool. Cameras photograph vehicle license plates as cars enter (being slowed by taking a ticket). The software of the system reads the license plate characters and compares them to a database. You may be able to use a police database and catch stolen or wanted vehicles. Alternatively, you can use your own database, which includes authorized vehicles, employees, and previous parking violators or unwanted guests. Your Marketing department can use the system to know when a VIP guest arrives and meet him in the lobby with his room key or a bouquet of flowers. Most importantly, a record of each plate coming in and out gives you evidence to be used in catching bad guys in their car or at least a time frame of when a car was stolen.

Speaking of stolen cars, having a booth attendant checking tickets as cars leave drastically reduces the chance of cars being stolen.

Security Patrol

Patrol type usually depends on the size of the parking area. Whatever patrol type you use—bikes, walking, vehicle, or perch—make sure they can cover the entire facility every hour or as your requirements dictate.

I recommend bicycle patrol for its speed, mobility, and stealth. Bicycles are relatively inexpensive, can get around almost anywhere quickly, and are a motivator for the more eager security officers. Bicycle officers must be properly trained and equipped (see Chapter 3). The Segway and other scooters might be used instead of bikes, but not as well.

Motorized security vehicles are expensive to operate and insure, but provide high visibility. This visibility is a deterrent, but also makes clear where security is not. Some hotels use a vehicle because this post tends to do double duty running errands. For inclement weather, it may be vital.

Walking patrol is the easiest to staff and maintain. Like the bike officers, make sure your officers outside are properly dressed for weather and visibility. They need to challenge suspicious persons and greet guests to provide that deterrence created by interaction.

Very few noncovered parking lots use a perch or elevated viewing platform, but they may be preferred in some areas. If you have one, staff it at all times. The false sense of security provided by having an empty perch could get you into trouble and the bad guys will figure out soon enough that it is empty.

Parking Enforcement

Enforcing parking accomplishes several objectives for your department and the hotel. The most important reason is the least obvious. Having officers looking for violators encourages them to patrol and keep their eyes open. (You have seen the rovers walking around in a daze or staring at the ground.) Enforcement also keeps the right spaces available for the right cars. You do not want employees parking in the premium guest spaces. You can use citations to discipline these employees or the annoying neighbors who use your lot without permission. Abandoned cars become more apparent when you enforce parking.

If you want to have teeth in this enforcement program, you have three options. First is the discipline, mentioned previously, that comes from an employee receiving a citation. Second, you can have a third party tow the vehicle. This gets the vehicle out of your lot, and costs the owner a lot of money to get his car back. The third option is a boot or immobilizer. This contraption secures one wheel so the car cannot move. It gives you a chance to confront the driver and explain the parking policies. You can use this opportunity to charge him a fee (which goes to your revenue instead of the tow company) and enter him into your database. This option is preferred because when you make a mistake—and you will make a mistake and boot a guest's car—it is easier to resolve than getting their car out of a tow yard.

CASINO SECURITY

Since the proliferation of gaming outside of Nevada in the 1980s, casinos are now in almost every state in the union and many other countries as well. Many of those casinos provide lodging as an amenity, so it is common to find a hotel attached to a casino. In fact, when casinos first started building large hotels in the 1970s, the hotel served two purposes. One was to get the casino patron to stay longer and spend more money. The other was to provide an amenity that the casino could give away to its patrons as a reward for losing their money. Of course, it also added some family aspect to a casino vacation where the entire family could stay and enjoy themselves while one or more parents participated in the gaming action.

Las Vegas, which has always led the way in gaming innovation and trends, built huge megaresorts in the late 1980s with the Excalibur, Mirage, and later, the MGM Grand. Each had more rooms than any other hotel in the world at the time they were opened. This competition ran off and on for a couple of decades and when the size of a hotel maxed out at about 5,000 rooms, they started building mini cities of several brands on one resort property. While the casino is still a large part of these destinations, it no longer provides most of the revenue. Retail, entertainment, hotel rooms, and even condominiums now contribute in a major way to the bottom line. In fact, even though big players can still get their free suite, most regular gamblers must divide their gaming expenses into lodging, food, shopping, and entertainment.

Casino security has evolved and changed just as much as the buildings in which they work. Security was originally hired in a casino to protect the money. The antics of casino security officers are legendary and depicted in movies as hired muscle that operated as the right hand of management to exact justice on those who would dare try to cheat the owners out of their money. These stories are a bit exaggerated, but only a bit.

In the 1970s as organized crime was pushed out by large corporations, the Nevada Gaming Commission stepped up its own enforcement of the casinos. Background checks became more stringent and the "good ol' boy" system all but disappeared. Regulations within the casino operation increased exponentially to prevent internal theft, which was allegedly committed mostly by management. Simple controls and dual and triple verification, accounting, and auditing procedures were enacted and enforced. This changed security's role from private thugs to protectors of assets. Ironically, the new marijuana industry is going through a similar stage. Their money is not allowed to flow through banks because banks are federally regulated, and marijuana is federally "Illegal." (Of course this could all be different by the time you read this.) I wonder how they are dealing with that.

Casino Controls

Casinos are now less corrupt and more corporate and have developed strict cash handling and accounting procedures. In a casino, most of the gaming money is uncounted. It has been virtually counted, but not physically counted, so it is most vulnerable. What casinos do, in almost every instance of moving money, is to use two or even three department representatives. One of these departments is usually security, not because they are carrying guns, but because they are the only ones left—or the only ones independent from the money. The first concept is Verification. Whenever money changes hands in a casino, a paper trail is created. Often, this paper trail is in the form of a receipt or slip that has to be verified. Security is often the second or third verifier of these transactions. If money is exchanged between party A and party B, a third, uninvolved person needs to verify it, so Security is used. This is not so much because of their job function, but because they are usually the only ones around who are independent of the money departments.

The second protection method in a casino is Surveillance. These professional observers watch employees and guests to identify theft, cheating, and fraud. They are mandated in most states to watch and record certain transactions and games. There are still some old surveillance guys around who actually crawled in the rafters of the casino, above the tables, to watch the players cheat. These same veterans have lived long enough to see great innovations in the size, range, and ability of cameras that allow them to watch from an air-conditioned office. As electronics have made the surveillance officer's job easier, it has also benefited the thief. Dozens of different methods of cheating have been tried and have succeeded over the years to gain an advantage in games of chance.

In our example of the pit fill, Surveillance watches the transaction at each step. When the chips are handed over to the Security officer, they are passed by a camera where the chips are photographed and counted and compared to the amounts on the slip. At the table, when the chips are again handed over to the dealer, Surveillance again photographs the chips and verifies the amounts. Even though the Security officer had possession of the chips alone during transport, they are verified at each end, narrowing the focus to him or her if any chips come up missing in the process.

One special place that Surveillance watches is called the count room. This is where all of the unverified money is taken each day to be counted. The cage is different; that is where money is exchanged, not verified. The cage maintains a balance of a fixed amount of money, never having more money than it is assigned until it receives a deposit from the count room. It never has less until it makes its own deposit to the company bank account. The count room does not have all of the controls and verifiers previously mentioned because it is receiving "raw" money from certain games and revenue centers. For this reason, there are multiple layers of security and numerous controls on this room. Surveillance is one of those controls and is responsible for making sure the other controls are followed.

In a casino, Surveillance performs many of the special audits and internal protection functions discussed in this chapter and Chapter 11. There are some great books dedicated entirely to casino security, some of which are by this same publishing company.

The third protection method in a casino is one that is discussed in Chapter 11—Internal Audit or Accounting. This department, independent of all others and headed by the aptly named Controller, is the final stage of all transactions. Auditors audit the transactions and make sure that everything balances, that no money is missing, and that all regulations and policies were followed through the other steps. This creates the final leg in the "checks and balances" of a casino operation. In that original example of a pit fill, an auditor would verify all three stages of that transaction the next day. The first and second copies of the fill slip come from the cage; the third copy comes from the count room where it was retrieved from the drop box on the table; and a fourth copy is the hidden or electronic copy contained in the cage records of money sent out. These are compared with logs of money coming in at the pit. The auditor also verifies all proper signatures on the slip, makes sure there are no sequentially numbered slips missing, and that fills requested match fills processed. There are several places, or a paper trail, to find exactly when an amount was changed, or a verifier missed.

Regulation Hierarchy

In Nevada casinos, and many other jurisdictions, the gaming authority will establish basic guidelines for certain operations. These are generally called regulations and they provide very broad mandates, such as: surveillance systems shall be "in accordance with the casino surveillance standards." Note that this does not really say anything except that there is some other standard you have to follow. That standard (in Nevada) says, "Access to a surveillance room must be … as set forth in its written surveillance system plan" (among other things). This puts a slightly tighter level of restriction on the casino, but it also transfers the remainder of the control back to the private entity. The government in this second level of control is saying, "You decide how you are going to control access, and then follow your own rules." Gaming Control will then audit you and enforce your own regulations against you. These are called internal controls. The next level is simply called house policy. For example, the Surveillance room may have a sign-in log or require an ID badge for entry. That is not required by a government agency, but it is your own policy for following the higher level of control. Then, to finish our example of these cascading regulations, the Surveillance department policy for entry to its room might be that officers only allow entry after verifying proper ID and with authorization from the room supervisor.

For better understanding, look at our own country's system of laws. At the top, we have the Constitution, which provides a broad framework to follow. The next level is federal laws, which give restrictions that are more detailed, but must adhere to the minimum set in the Constitution. The next level (generally) is the laws of each state. The state can have a law that is more restrictive than a federal law, but not less, so they are usually just more specific. Then we have local ordinances and even private property policies.

I explain gaming laws in this manner to illustrate that most rules that we follow in a casino are not really laws at all. They are often house policies put in place to make sure we follow those broad laws and regulations. This is important when enforcing and following rules. It is also helpful to know that because most of the procedures that officers follow are created by the casino, they can be changed by the casino. If you are doing a pit drop at 2 a.m. every day, which also happens to be the closing time for all the nightclubs in your area, you might want to change one of those times.

Casino Patrol

Besides the previous examples, Security provides many more administrative and regulatory functions in a casino. This includes drops (removing money from a device), escorts, transfers, and key issuance. Security also patrols as outlined in this chapter. In addition to normal protective patrol, they also are responsible for keeping minors off the gaming floor, addressing those suspected of fraudulent acts (e.g., taking money from a machine without placing a wager), and enforcing alcoholic beverage laws.

Some jurisdictions do not supply free drinks or allow smoking as they do in Nevada, so alcohol is a major factor in most security-related issues in casinos there. Security officers need to be specially trained in recognizing intoxication as well as managing those who have had too much. Even though Nevada's dram shop laws (more detail is in Nightclubs and Bars in this chapter) place responsibility on the person doing the drinking, casino Security officers are very aware of their moral responsibility in handling intoxicated persons. We no longer see officers throwing drunken patrons out the back doors into the alley. Sensitivity and responsibility have prevailed and now officers will go to great lengths to protect an intoxicated person. This may include taxi service, phoning a friend, all the way up to providing a room (for good players). This is good business more than a matter of legality.

Casino security officers need to be specially trained in cheating laws in their jurisdiction. This brings us to the difference in Surveillance and Security. Many people confuse and even merge these two casino functions—probably based on movies and television. Like everything else, properties vary, but the differences are fundamental and very clear. Surveillance reports directly to the Controller or General Manager. They are an oversight department like Accounting and have to be separate in the chain of command from Security. Surveillance is the "eye in the sky," primarily watching anything that has to do with gaming, money, or compliance. I say "primarily" because more and more, Surveillance departments are using "dataveillance" to watch their assets. They have the unique ability to take a transaction from an exception report in the accounting system and actually observe it live or recorded to see what really happened. A good Surveillance department uses any tool that it can get to catch internal and external theft and fraud.

Security in a casino is the more visible representation of enforcement and prevention. Security physically patrols and responds to incidents of all types. In fact, if Surveillance sees a crime in progress, they will generally call in Security to make the arrest or detention. Security also may monitor certain cameras, but usually they are related to guest and employee safety, such as the common areas, access points, garage, perimeters, and stairs. Some jurisdictions—not Nevada—have a gaming agent who is actually employed on property to ensure compliance and enforce gaming laws. So, in these cases, Security may have nothing to do with a gaming crime because Surveillance will work directly with the agent in-house.

Detention

Also in Nevada, and in some other states and tribal areas, gaming laws allow for "detention" rather than arrest. For example, if a Security officer has reason to believe a person committed a gaming crime, he may detain that person to notify a gaming agent. Notice the difference is that they do not have to know a crime occurred or even witness it. This protects the casino from liability and allows the gaming agents to perform an investigation if they merely suspect a criminal cheat. The example in the textbox below shows the abuse of this enforcement tool.

In 2010, a guest at a large Las Vegas casino was suspected of cheating at a table game. Security followed the man to his hotel room, detained him, transported him to a holding room, searched him, and took $500 in gaming chips that the casino would have won if the bet had been completed. Security then "trespassed" the man and evicted him from the hotel, never notifying a police officer.

Although most gambling jurisdictions have special laws designed to assist in the investigation of cheating, there are no laws that can trump a person's constitutional rights. This "arrest" violated federal law, state law, gaming law, and even the casino's own policies. As usual, the $500 return on this situation will not even come close to the likely settlement that will be made.

Deployment

Deployment of security officers depends entirely on the size of the casino and what other facilities it has, such as hotels, restaurants, shopping, and parking. In the old days, the priority was on the money and all you saw was an officer stationed near the cashier cage and the rest of the officers moving money about the floor. As we have evolved, we realized that money is an asset secondary to our guests' safety. Now most casinos have officers patrolling the floor, perimeter, and other areas watching for troublemakers and preventing problems.

If you have a casino on your hotel property (or a hotel on your casino property), you likely have a done a Risk Assessment and made a Security Plan as described in Chapters 1 and 2. You also know that the money in the cashier cage is insured and worth far less than a rape or a physical assault in your garage. Besides, your cage robbery procedures probably instruct cashiers to give robbers whatever they ask for to protect employees and bystanders. However, there is at least one simple thing you can do to increase your patrol coverage or reduce your workforce. That savings comes in the form of all of the regulatory functions that you provide. This requires some collaboration with other departments. See if you can schedule all of your drops and other duties in a sequential format. For example, instead of starting the pit drop and the validator drop, try to change the start time of the pit drop to be first, then the validators immediately after. Most casinos used to schedule four officers (or more) at that one hour of the shift just to complete those tasks. Only two are needed if scheduled sequentially. I once knew of a very large casino that scheduled 12 officers between 2 a.m. and 4 a.m. just for drops. The controller wanted everything in the casino dropped simultaneously to make the paperwork look cleaner. Someone finally convinced this controller that the cost of security for this daily event far exceeded whatever convenience it was for the accountants.

Innovation

Casinos invest more than the average business in surveillance and detection equipment, hire and train teams of officers to staff surveillance rooms, and have unusual situations and crimes. Therefore, the casino industry has given the rest of us many innovations and methods that we might have never encountered.

For decades, Security Departments placed cameras in a manner that allowed us to get a great view of the top of customers' heads. We have since learned that we can get better images of faces from cameras mounted at a farther angle on the ceiling or even mounting them on the wall and in doorsills. Casinos are also very good at using what are called "choke points" and high traffic areas to get identifiable shots of perpetrators. An overhead camera can get a view of a certain activity and then a camera placed in a high traffic area can be used to identify the person. Despite what you see on television, facial recognition has not been refined to a practical application, but casinos are getting very close. I suspect they will be the first to master this emerging technology.

Casino surveillance officers have perfected the science of video patrol and investigations. These experts have developed techniques that maximize the power of video. Where we used to use video to passively monitor a particular area, casinos have taught us to identify suspicious behavior, zoom in on it, and use multiple angles to determine criminal behavior or undesirable activity. There is more information on video patrol in Chapter 12.

Casino accounting departments regularly use video to audit gaming. They may use it to recall a Keno game or verify a large jackpot. In casinos, it is very common for a department head to have a video feed right to her office to monitor her employees and customers.

Casinos have also taken inter-property communication to levels that are more effective. Besides just having meetings where suspect and criminal information is shared, they have gotten very good at transmitting this data in real time to their neighbors. Video links, Internet streaming, and email are just a few of the ways that casinos can send images up and down the "strip" before the bad guy even gets to his next destination.

There is no patent or ownership of these ideas and techniques. Take advantage of this experience and utilize these concepts wherever you can find them useful in your operation.

MEDICAL

Our medical abilities have been changing over the decades. Privatizing EMTs and deploying AEDs or PADs (Defibrillators) are just the beginning. Many of you are already carrying and administering Naxolone. This drug has been around for more than 50 years but has more recently been used as an opioid overdose "antidote." Also known as NarCan, it is available for emergency use in an inhalant. Though you must ask a pharmacist for it, it does not need a prescription. What it claims to do is increase breathing for patients that have consumed more than 100 mg of an opioid. What it actually does is cure everything except COVID. We looked at this product before we added it to our ambulances years ago, then we saw it work. The paramedics use it so often, they keep it in their shirt pocket. If you ask them, they will tell you that it works on more than just opioids and more than just breathing problems. This is a good thing and health departments are now encouraging groups like Hotel Security departments to carry it. Wow! Really? I remember when we could not apply burn gel because of the liability concerns. Now we are administering drugs? Actually, it is a minor drug, as drugs go, because most druggies are not interested in it.

So what is next? I see technology carrying most of our medical advances, as it does everything else.

6

Physical Security and Crime Prevention Through Environmental Design (CPTED)

With Contributions by Russell Kolins, CPP

Physical Security is just about everything that is not in the Cyber Security toolbox. If you are reading this book, you likely know more about the former than the latter. Since the parts and pieces of Physical Security have so many applications and combinations, ASIS and others have organized them into what is called the Physical Protection System. (I will explain later why this matters.)

It took me some time to buy in to this way of organizing what we do, but now that I completely understand it, it makes perfect sense. The Physical Protection System (PPS) does not give us the solutions, it just provides the framework, so we have everything covered. You can operate without ever referring to the PPS, and likely end up with the same result, if you know what you are doing, but the PPS ensures that everything is covered. The PPS divides all physical security measures into three categories and are explained as follows:

Personnel—This category obviously covers the humans that have a role in the protection system. More than just security officers, it may include other employees, the police, inspectors, and anyone else that plays a role in protecting this particular asset. Human resources have been introduced throughout the book under the headings of training, hiring, deployment, and are woven into other chapters as well.

Policies (and Procedures)—Any policy that is related to the security of the premises is in this category. It may also include signs ("no entry"), Codes and Ordinances, and Training. Note: I put Training in this pile instead of the personnel category because the documentation of training is as important to the system as the actual training itself. Policies and procedures are also woven throughout this book under the chapter of the same name, but also in other chapters where relevant.

DOI: 10.4324/9781003037644-6

Resources—(If you are looking for another "P" word here, perhaps we could use "Physical," but I was always taught not to define a word with itself.) This category is all of the "stuff" we use for the PPS from rocks (used as bollards) to alarm systems to guns and lights. …Which is a good segue into CPTED, but not quite yet.

If you have been doing Physical Security for any amount of time, there is little that is new here for me to show you. But that is not why I am here. Recall in the first chapter, we talked about a Risk Assessment leading to a Security Plan. The Security Plan should make up the Physical Protection System. This is important for two reasons. Most importantly, the PPS provides a framework, or stencil, if you will to make sure you do not leave anything out. For example, if you are trying to keep a parking garage safe for those who use it, then you might install cameras, walls with locked doors on the perimeter, limitations on who can use it and when, and post signs like "lock your car" and "No loitering." That would be a pretty comprehensive system except it leaves out the third leg of the triangle, which is "humans." You are thinking security officers patrolling—and you would be right—but there are other humans that have a role in the safety of that garage. They include: someone to monitor the cameras live, parking attendants, the cleaning crew, employees passing through, and even the police who do a drive-through on occasion. In the past 20 years we have even learned to "deputize" the humans that use the garage to help us protect it. This is best exemplified by the "See Something Say Something" campaign. What better person is there to notice something out of place than the person who uses that place every day?

The second reason—which is almost as important as the first—is as a liability defense. If some fancy Security expert like Russell Kolins, who I will introduce shortly, is called in to scrutinize your garage security on behalf of a victim of a violent crime, one of his first observations will be the PPS. Digging deeper, he will opine as to whether you took every reasonable step to protect the victim that was known or available to you. Leaving out something like security patrol, might be plenty for him to show that you are indifferent to the safety of guests.

Note that this book is loosely organized around the system I just described. It starts with policies and procedures, then transitions to personnel with conduct, training, patrol, etc. The remaining chapters are more or less the resources that we use. Until this stuff becomes second-nature to you, I suggest making a simple table with the three columns every time you plan any event, remodel, new construction or whatever. It will help to make sure you are not relying on any one component or leaving anything out.

The remainder of this chapter centers around the physical security measures one might use in the hospitality setting. These are not all inclusive, but can give you an idea of the tools you can use.

CPTED

Crime Prevention Through Environmental Design is a science that is somewhat young, but has its foundations in design and architecture going back centuries. I called upon a friend and colleague, Russell Kolins, to explain a bit more about it. Kolins teaches CPTED at the university level and is thereby more qualified to introduce it.

Crime Prevention Through Environmental Design, by Russell Kolins

CPTED, pronounced SEP-TED has been around as we know it for about four decades, but in reality, CPTED as we didn't know it by that name existed long before it was named by criminologist, Prof. C. Ray Jeffrey as crime prevention through environmental design. (Oscar Newman, an architect, created the concept of defensible spaces—*Defensible Space*, 1972.)

The initial idea surfaced when a journalist, Jane Jacobs, wrote that physical environments could be used to reduce crime.

There is so much more history involving many professionals, professional organizations, and police organizations that work with the professional organizations that recognized CPTED as an international standard for crime prevention. In fact, just recently, the international CPTED Association announced an ISO standard that the ICA helped to develop.

All enforcement agencies began to realize that using CPTED measures, the crime level was reduced in their communities so much so that the University of Louisville, Southern Police Institute (SPI), teamed up with husband and wife CPTED practitioner pioneers, Stan and Sherry Carter, to develop a college course, CPTED, taught in one week sessions four times a year at the University. The course is popular with security personnel, government representatives (federal, state, county, and local), plus all four branches of the military. The University and SPI is also contracted by police departments from around the country for the class to be taught to their agency in-house rather than to bear the cost of travel for the many officers and local government officials to travel to Louisville.

The International CPTED Association, ICA, was founded by Greg Saville, Barry Davidson, and Paul Wong in 1996 as a professional non-government organization dedicated to implementing CPTED around the world. Today, the ICA currently has a membership of over 233 countries including security professionals, police, planners, architects, developers, academics, and others interested in safety and security planning using CPTED. The ICA mission statement is "to create safer environments and improve the quality of life through the use of CPTED principles and strategies."

Let's look at the CPTED principles and strategies and how they apply to the hospitality and entertainment industry, but first, it's important to know the more formal definition of CPTED by Thomas Crowe in 2000.

Crime prevention through environmental design provides that, "*the proper design and effective use of the built environment can lead to a reduction in the fear and incidents of crime and an improvement in the quality of life.*" In other words, CPTED reduces the opportunity for people to do bad things and engage in inappropriate behavior. CPTED further promotes positive social interaction among the good people using your space. It all boils down to ***prevention.*** Obviously, there are many moving parts that factor into the equation of prevention as have been discussed in previous chapters, but let's find out how and why CPTED is an efficient and cost-effective preventive tool.

Kolins makes another contribution in Chapter 10.

******

CPTED: Crime Prevention Through Environmental Design is the concept of incorporating the Physical Protection System into the design, architecture, and landscape of the asset.

Some refer to this as Defensible Space, which is fair, but not quite as advanced. Mr. Kolins, who teaches CPTED at the university, police and corporate levels, shows us in Chapter 10 how establishments with alcohol service can get the most out of CPTED to protect themselves, their license, and of course, their intoxicated guests.

Meanwhile, I am going to review some practical applications of CPTED that are common in the Hospitality field. As I have mentioned throughout this book, if you do not employ these concepts, prepare a good reason, because you may have to explain why. CPTED does not get all of the credit for our protective measures but deserves some for advancing the concept.

Frankly, the hospitality industry is new to CPTED and physical security. Because we operate "soft targets," we traditionally did not need much more than a lock on the back door and a hotel detective to keep the peace. In my mind, there are three contributors to our need for physical security in hotels and the like. One is simply, changing times. You may think this a default answer, but generationally, our security posture is changing. As crime rates go up and population fills in the blank spots on the map, we are now locking our doors at night, growing warier of strangers, and so forth. This is not a commentary on anything except that, "Things ain't what they used to be." The second prong of my theory is Terrorism. Way back to the Gulf War (and probably before), I was going to seminars given by the Middle East security professionals who had gun turrets on the roof, metal detectors at the doors, and difficulty hiring employees for fear they would be insider threats. And these were hotels!! Needless to say, this environment has crossed the waters to other countries who make their soft targets pretty hard to hit now. (If you have not heard of the Mumbai attacks, it will give you some insight as to how vulnerable we can be. Check it out.) Finally, the hotel experience has changed from a societal benchmark into one that attracts a younger, more diverse, customer—including criminals like pimps and traffickers who find it much easier to do business in a hotel.

The casino I worked at in the 1990s had been open for about 20 years when the first civil disturbance occurred just outside its main entrance. This was a full-fledged riot with police cars being overturned and everything. The call came out from the police to "lockdown" the casinos and only allow entry to hotel guests until the ruckus could be cleared. No problem, except, well there was a tiny problem: our doors had no locks. They were designed and installed intentionally with no way of locking them, and so for 20 years had remained unlocked. We had to makeshift some chains and other hardware so they could be secured. The following day we had contrived some gadgets that attached to the doors on the inside so the doors could be temporarily locked.

Enter Physical Security: That's us. CPTED gives us a great way to meet the challenges of security sometimes less expensively, certainly more aesthetically, and without making guests feel uncomfortable. Following are some common security measures used in hotels and motels (and elsewhere). If you are not deploying these, ask yourself why and then proceed accordingly.

Exterior Physical Security

The exterior of our property is often neglected because it is "out of sight," "part of the street," not where our problems are, or any other excuse one might create. I believe the opposite of those statements is true. Guests, and criminals alike, must approach our building, park and check things out before ever approaching a door. You can see this for yourself by looking at certain hotels. You can see how some of the big chains—that study and invest in CPTED technology—present themselves to the public using standoffs, effective lighting, parking design, and other principles. Following is a brief list of some of these principles that I suspect are known to you, but when do you see them all together at a lodging property?

Landscaping

Landscaping is a broad topic as it applies to CPTED and includes some of the topics covered elsewhere in this chapter. Generally, what I will try to explain here is how the gardening around your facility deters criminals and makes guests feel safe. The idea is to make entries and approaches inviting while keeping vulnerable areas off limits. Here are a few of the many ideas being used. You can come up with your own also.

Certain bushes have thorns or sharp leaves that prevent someone from easily climbing over or around them. These are ideal near windows. Besides a physical barrier, bushes are used as concealment. The opposite also applies that you do not want your greenery to conceal a burglar or other undesirable person near the windows. Note, for example, how hedges are used as boundaries, to hide walls and fences, and as the wall itself.

Trees are a great addition to landscaping, but they should be kept trimmed so as not to block sight lines that should not be blocked. They can also block lights and cameras if not maintained.

Walkways—The area surrounding a hotel or motel should have clearly defined pathways. Shrubbery should be kept trimmed so it does not block paths. The paths should be as smooth and accessible as the indoor hallways. Luggage, wheelchairs, strollers, and high heels do not do well on stepping stones, sand, or gravel. Cracks should be repaired as soon as they alter the level of the surface.

Standoff Area—Another aspect of CPTED is to have a distance from the property line to the entrance that allows for some delay and detection. An approach to the main entrance allows employees (and guests) to observe and evaluate visitors before they get to the doors. This gives time for the observer to decide if they are going to challenge the visitor. In the case of a guest observer, it gives them a chance to stay behind locked doors until the person proves himself to be legitimate—with a room key, luggage, name tag, etc. A standoff area should be attractive, functional, and safe. Lighting is important and there should be no hiding places or obscured sightlines. Standoffs are a concept borrowed from the military. If you have ever driven on to a military base, you might have seen traffic-slowing devices, clear landscaping, positions of observation, cameras, lights, etc. The difference in a hotel is that we design it to look natural and inviting.

Sight Lines—When space limits the amount of standoff area and open space, there should be clear sightlines to reduce “hidden spaces.” Following simple CPTED recommendations will ensure that windows are not blocked, stairwells are visible from outside, and that ingress points are visible from the office, rooms, or common areas. If you have ever seen a parking garage where the stairwell was exposed by windows, that is CPTED. The elegance of CPTED is that it contributes to safety and beauty at the same time.

Cameras—Cameras that capture and record activity are good investigative tools but do not prevent crime. Properly placed cameras that are monitored in real time can be an excellent detection method. Inexpensive technology exists to see in the dark, alert the user to motion, detect unauthorized persons, and even spot criminal behavior. The price and simplicity of these systems make them a must in the hospitality environment.

Patrol—It may not be practical to have a full-time security officer watching the perimeter of a motel, but there are other ways to fulfill this obligation. Hiring a private patrol company to make regular rounds of parking and perimeter areas adds another layer of security. The patrol company may also be able to respond to suspicious activity faster than the police and without becoming a nuisance to the police. At the very least, an employee (or patrol) should make a visible check of the exterior every one or two hours—depending on location and size of property.

Parking—Parking areas should be strictly limited to guests only. Unauthorized and suspicious persons should be challenged and dealt with immediately. No loitering policies should be posted and enforced. This includes loitering by guests. Abandoned and unauthorized vehicles should be towed as soon as possible (broken window theory). The parking area should have as few access points as possible to prevent escape, hiding places, and being used as a pass-through. Proper fencing or other CPTED measures should be in place to make sure the parking area is accessible only by a visible and controlled ingress/egress point.

Building Entry—Access to the building, especially after hours, should only be at doors that are constantly monitored by a human. Since most motels have limited staff at night, the front entrance is generally the only door accessible by guests. Attention should be given to fire exit requirements. I do not recommend locking back doors if those doors are the closest entry to a parking area or back entrance. This may limit a guest's opportunity to seek safety if they are confronted outside, followed to the motel, or see someone suspicious in the parking lot. These ingress/egress situations should be addressed case-by-case but should always take into consideration safety over convenience.

Motels tend to have exterior hallways with unchecked access to room doors. Lighting needs to be adequate to illuminate and prevent persons from loitering in dark shadows. Shrubbery should be trimmed so that it does not obstruct the view of the hallway. Non-guests need to be challenged and dealt with properly. Avoid having accessible rooms for vending, ice, and supplies. Lock storage and maid rooms but keep ice and vending in plain sight with unobstructed views. Secure gyms, business centers, pools, and other common areas after hours unless they can be monitored by a human.

Outside Safety—Guests tend to wander off property after hours for exercise or to go to a convenience store. It is best to eliminate this need by providing exercise facilities and sundry items for sale (at a reasonable price) so guests will stay in the building. The second-best option would be to provide escorts or shuttles to and from certain destinations. The third best practice would be to provide a list or map of preferred destinations or jogging paths.

Smoking Areas—As local smoking laws are followed, it is important to make sure the guests and employees in these areas are safe. (1) Keep guests and employees segregated (two different areas). (2) Make sure these areas are not "hidden." (3) Watch for non-guests using these areas and approaching guests. (4) Have someone assigned to police used butts to keep vagrants and intruders from loitering there. (5) Frequent checks, adequate lighting, camera coverage, and panic buttons should be considered. (6) Do not install benches so as to discourage loitering.

Music—It is not often we get to use our sense of hearing to prevent crime. You may want to consider a study in the last decade in Paris, France. Researchers, trying several types of sounds and music concluded that music—specifically vocals—made persons feel safer than they would in an otherwise scary-looking garage or lot. Some businesses take this a step further and blast classical or opera music which helps to ward off gangsters and other loiterers.

Lighting

Photometrics—Yes, that's a thing—is about the measure of light. All we knew when I was growing up was "watts" which, or course, is just the power consumed by a lamp. But now that lamps do not all use the same tungsten wire that Edison mastered, bulbs of similar wattage can produce widely varying heat, color, and brightness. Other metrics have been introduced to us to compare lights of different types and you may find them useless, but there are architects, engineers, designers, and lawyers who base their careers on them. So here is your quick start guide to lighting.

Lumens are the measurement of light being produced by a lamp. We used to go by wattage but we cannot do that anymore because a 6 watt LED is brighter than a 40 watt incandescent bulb. So the more lumens the brighter the light. Light efficiency is generally measured by lumens per watt. LEDs are considered the most efficient because of their very low energy consumption.

Candelas (Candle power)—If Lumens is the amount of light emitting from a lamp, Candelas is the measurement of light that lands on the wall. For example, a high intensity flashlight would have high candlepower with a modest number of lumens. A laser hardly has any lumens but a large candle power number. On the other hand, a stadium light which has a huge number of Lumens and covers a large area, has a low candlepower. The sun: a gazillion lumens, wimpy candlepower. Also note that lumens are affected by the amount of energy and type of bulb while candelas are a result of refraction, mirrors, diffusers, etc. That cool flashlight you carry at work has a low lumen LED bulb powered by about 3 volts and by the time it is intensified with mirrors and aimed close to a wall, it is brighter than the sun.

Lux is one lumen per square meter. This number (and foot-candles) is a number applied to certain areas for the purposes of standards or building codes. Now we are getting into some security stuff. A jurisdiction may require, for example, that the lighting in a parking garage be five foot-candles at the most. A kitchen, by comparison is more like 50 foot-candles (OSHA measures in foot-candles). Most countries on the metric system use lux.

Because lux or foot-candles are the result of wattage, lumens, placement, and so forth, you cannot buy a light that is 5 or 50 foot-candles. A photometric study needs to be done to determine the lighting needed. There are people with expensive devices that can do that. Foot-candles: hmmm, so we may be at a liability if our foot-candles are not up to a standard and someone has an accident or is attacked in the garage. Now we are talking security. It is helpful to know when the facilities folks come along with some money-saving light fixtures.

Light placement—Ever wonder why lights are mounted on the ceiling and not the floor? Me neither, but it's an interesting question. First of all, foot-candles are measured on the floor usually (or the walls) so lighting from above is necessary. But from a practical point of view, the floor is where we walk and the surfaces are where we work, so light from above is where it's at—literally.

Indirect lighting is simply a method of lighting an area without the light source being visible. "Washing" a wall or ceiling provides illumination of an area without the light being the focus of attention. Many fixtures can accomplish this for us. Even track lighting that is designed as a flood light can be pointed at the wall to create indirect light.

What about up-lighting? Up-lighting, oddly enough, is lighting that points up from the ground or a lower wall. This is a method of indirect lighting because although the ceiling or wall is directly illuminated, the source is not visible. This is a common technique in exteriors and landscaping. Huge buildings do this, but houses, apartments, and hotels do this for reasons besides diverting attention. Besides the aesthetics of lighting the exterior from the ground, this method of indirect lighting creates backdrops and ambient light for safety. For example, a floodlight that you tend to see on the eave of a building pointed at the driveway accomplishes the illumination of the driveway but also interferes with one's visual perspective. A bright light shining at you makes you want to look down or away. It is not pleasing and takes away a good portion of your most important sense. A light pointing up at the side of the building creates a backdrop that will attract us and guide us while still providing indirect light.

Speaking of flood lighting: I suppose we could call it down lighting, but the term flood alludes to the fact that it is intended to flood the area with a lot of light. Again, not very pleasing unless carefully placed so it is not in the viewer's eyes. Generally, more than one flood is better to reduce shadows. Stage lighting uses multiple fixtures at different angles to reduce shadows.

Diffused or shaded lighting is a technique used to aim or control the intensity of lighting. A simple example of this is a lamp shade which allows a flood of light on the table surface, a flood to the ceiling and diffused light to the sides. Sconces on walls tend to provide the same effect.

Color Temperature—The "white-ness" of light also has a measurement. It is measured in kelvin as if it's a heat measurement, so the number is arbitrary and relative. Daylight or a fluorescent light in an older office building is about 6,500k (darned white). The incandescent bulb in grandpa's reading light is about 3,000k. When you purchase light bulbs these days you need to check this number depending on how the bulb will be used.

Use of Color—Cool white, soft white, and other such terms make us think of light as something that affects mood. This is an understatement. We associate bright white with work and energy and business. Candlelight is romantic and quiet. Golden light or soft light is used in model homes and some businesses that want the environment to feel warm and cozy. Jewelers use extremely bright light in the cases to accent the sparkle of the gems. It is interesting to see how designers use light (or lack of it) to enhance whatever business they are promoting. We too, in Security can use color or temperature in the same ways.

Shadows—Just the mention of shadows is spooky to some people. At night in a strange area it makes them feel uncomfortable. When you think about it, though, it's also a distraction. Someone who is walking through a parking lot with one big floodlight sees a shadow from a tree or a person or car and it breaks their concentration. It gives their eyes something more to investigate. Imagine watching your favorite game at your favorite stadium and there is one really bright light illuminating the entire field. The shadows of moving players would drive you crazy and distract from the game.

Put It All Together

Let's look at a few examples of lighting in a hotel setting.

Imagine a garden path behind your hotel. Backdrop lighting or wall washing might be used on the exterior walls to show the boundaries of the space, expose anyone that would want to lurk there, but softer tones and temperature that tell the viewer this is a backdrop and nothing to see here. Up-lighting of trees, large shrubs, and fixtures highlight the ornamental value of those objects and show the observer that it is not a person, and no one is hiding there. The walkway itself is the focus of our canvas so it has either waist high low intensity floods to light the way or draw your attention to the way you want to go. If the up-lighting of the trees is not sufficient to provide enough ambient light to see faces and bodies, then some overall down lighting would be necessary.

The parking lot is a little less subtle and decorative. When we talked about Risk earlier we decided that the parking lot is pretty high on the list of places that need a lot of attention. Unlike a garden walkway, we are not going for mood here, but high security. The more light and less shadows the better. High temperature floods are the way to go. If you notice almost any parking lot anywhere, the light is white, bright, and very high on a pole. That reduces shadows. A bright light that was only 10–20 feet up would cast longer shadows the farther you were from it. High lights, properly spaced are standard (and probably a building code where you are). If the lot has walls around it or a building adjacent to it, consider washing the wall with light. Again, this avoids shadows.

Many times, litigation around an accident or an assault can come down to the lighting. Was it reasonable or sufficient to prevent the incident? Lighting at the site gets compared to industry standards, local similar venues, and building codes. A lighting engineer or designer can tell you if your lighting is satisfactory and how best to achieve what you need to have. At the very least, you should do some "reasonable person" tests. Check these lighted areas and make sure you can see persons lurking, exits, hazards, walkways, etc. If you cannot, you can bet this will be one of the first deficiencies attacked by your opposition.

Physical Barriers

If there is any way for a car to crash through any of your doors, you need to block those doors now. Too many prior incidents have occurred to ignore this risk.

During the first gulf war in 1990, a hotel in Reno was operating at a quick pace with a line of cars stretching from Valet to the street, causing traffic jams and some heated tempers. As the cars were inching their way to their vacation, one man in a Cadillac had a heart attack. His foot mashed on the gas pedal and the car went speeding straight into a set of doors, instead of turning left with the driveway. The metal framed door (like you see in most malls or retail stores), easily gave way as the Vehicle Borne Senior Citizen Device crashed through the two sets of doors, past a dozen slot machines, and came to rest between two blackjack tables.

The reason I mentioned the Gulf War is that tensions about terrorism were a little high and most people thought it was a deliberate act. There were no serious injuries or deaths, but the response and business continuity for the entire area were tested, with one zealous official calling the local military bomb disposal guys "as a precaution." The ironic thing was that a waist-high concrete planter, which would have stopped the runaway Cadillac, had been removed months prior for the sake of aesthetics and open access. But wait, it gets better.

A couple of years later, no modifications had been made to the entry because the thought was "what are the chances of that happening again?" This time, the exact same thing happened, except it was a Lincoln, not a Cadillac. If you read the early chapters, someone would have been on the hook for the blame as that second one was foreseeable. This is one of the best examples of how a foreseeable incident shifts the blame to the hotel.

Are you ready for the Chrysler to crash through the doors? No such luck; however, would you believe it took several more years for those doors to be protected by bollards. To this day, the employees call that particular access point the "Cadillac Doors."

The inset story highlights the use of bollards. Bollards come in all sizes and types. You may have seen the moveable kind that functions like a gate and collapses on demand to allow vehicles to pass, or that stays down and pops up when it perceives a threat. Those are more practical for military installations and even rental car facilities. Most hoteliers do not want a steel gate to represent hospitality, so CPTED calls for more discreet barriers.

Bollards not only keep cars and trucks where they are supposed to be, but also have to find a balance between efficacy and aesthetics. Instead of seeing steel blocking structures at hotels and resorts, you are more likely to see something more discreet like rocks and planters. There is a difference in markers and bollards. There are venues that use light standards or lane markers to separate pedestrian from automobile traffic, but these do not prevent the intentional or accidental crossing of those boundaries.

Designers and architects have come up with some clever bollards that meet our requirements without being obvious. Take a look around and you may see spherical concrete "balls" adorning the entrances of a retail store, or obelisks that are both decorative and functional. The most interesting ones I have seen were planters that were smaller at the bottom than at the top. These planters are top heavy, so when struck by a vehicle they topple easily, creating a wedge that prevents the vehicle from going much farther. Then there are simple steel pipes filled with concrete inset in the ground that are tried and true. Whatever the solution, I recommend doing something in this regard as it has happened enough times to make it foreseeable.

Walls and Fences

The difference between these two security tools is substantial. A fence is generally wood or metal, see-through, and used more as a visual boundary than a physical one. A wall is built for strength, obscurity, and as a physical blockade. Walls are usually concrete, masonry, or even rocks. Earthen berms are neither walls nor fences as they can block sight, but little else.

Just like cameras and lights, your decision to have a wall or a fence is dependent on the application. You would use a fence as a deterrent that reminds people not to go past a boundary. Public swimming pools are a great example of the use of a fence. A fence around a pool allows people to see in and out of the pool area for safety. It also provides a more open environment where guests do not feel enclosed. (Note that hedges and trees are a better compromise for privacy.) Fences are also used as concealment, like around the pool pump or an air conditioning unit. As for the perimeter of the hotel, you will have to determine what the objective of the barrier is. If it is just to denote a property line, then a fence may be fine. If your neighbors are other hotels, you may skip the fence entirely and leave it open. This allows for overlapping security where the neighbors can watch your parking area and you can watch theirs. If the hotel is up against a residential area or the back of a retail or commercial area, I would recommend a wall that is difficult to climb. These back areas are where car burglars and assailants tend to enter and once locals identify your lot as a shortcut (through a gap in your perimeter) your crime will increase.

Of course local building and zoning codes may decide what type of barrier you use and how high it is, but even those can be waived in the name of safety.

Conclusion

There are not many architectural solutions discussed here because presumably your building already exists. If it does not, please consult a CPTED expert in the design phase of new construction.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

7

Emergency and Incident Response

MAJOR EMERGENCIES

Emergency response is more than just awareness. It may become necessary for employees to participate in the response to certain major incidents. Fire alarms, active shooters, earthquakes, and hurricanes involve every occupant of a building. In most of these and other situations, security staff will be overwhelmed and will need as much assistance as possible.

This should be incorporated into your emergency procedures. Security officers will perform the critical functions, such as responding to the scene of the fire or cornering an active shooter. Bell persons can lockout elevators and evacuate the lobby. Food servers can clear restaurants. Housekeepers can check hotel rooms for stragglers.

Most employees, when presented with the idea that they are necessary and part of the team during emergencies, will respond eagerly and proudly. For those employees who might resist new job duties, it may be necessary to remind them or their department head of the gravity of these situations. Nobody wants anyone injured or killed during a disaster or violent incident, especially if he could have been saved if it was not for the inaction of an employee. Besides that, most normal operations, such as delivering luggage and serving food, will cease during an emergency, so employees' regular jobs are suspended until the emergency is over. They may as well help with the emergency until it is resolved.

Your response procedures to every emergency are going to be unique to your property, your staffing, and your policies. Rather than write these procedures for you, I have outlined some things you should definitely include, some suggestions based on my experience or that of others, and some cautions of mistakes others have made.

As I have mentioned every step along the way, start with your objective before making a plan. If the building is on fire, is putting out the fire your primary objective, or is it the safety of your guests? (Right answer: guest safety.) Once you have that objective figured out, decide how you achieve it. Based on 100 years of history, evacuating is the best practice. And what are the procedures for evacuating? Use alarm, public address, and door-to-door contact. Now you can write those procedures. Who goes where, who does what, etc.

DOI: 10.4324/9781003037644-7

Fire Alarm

In the United States, it is unlikely that guests in a hotel will die from a fire in that hotel. That is because we have been trained what to do since we were five years old. Line up and evacuate, right? There are some other reasons for safer buildings: Fire Sprinklers, earlier detection, advanced firefighting, etc.

Unfortunately, I can (and will) still give you many examples of death in hotels, restaurants, and clubs due to fire. In fact, often it is the evacuation that kills—not the fire. What you do not want is for your staff to rush to the tenth floor where the alarm is sounding while guests are making their way down the fire stairs on their own.

If you have not already done so, get with your local fire station captain and find out what their role is when the alarm sounds. It is kind of like an active shooter where the police are going after the threat while you care for guests. Although the Fire department is concerned with life safety, they may have different priorities and methods, so find out what they need from you. In a large structure, your job will be to update them en route with size and scope of fire, if any. Your job when they arrive is to show them the fire command center and supply them with resources they need such as master keys, rooming lists, schematics, etc.

Many jurisdictions now allow for a two-stage alarm signal. The classic is bells and sirens or strobes to tell people to evacuate until it is reset. The two-stage, used in buildings with a full-time staff, allow for that first stage, and then once the alarm is acknowledged by an authorized user, it goes into a second alarm, which may be an announcement like, "We are investigating the fire alarm you just heard. Please standby for further instructions." This reduces panic evacuations and the unnecessary evacuation for false alarms.

In my experience, the biggest hazard during a fire alarm is not the fire. It is the movement of hundreds of persons to a safer place—the evacuation. The challenge is not only volume of persons, but the "means of egress." The good news is that you can correct some of these challenges now and not wait for an evacuation to find out how dangerous your egress is.

Chicago 2003: A nightclub filled to capacity at about 2 a.m. experienced a fight in which security used pepper spray. The cloud of irritant spread through the dance floor and caused a panic rush for the door. Hundreds of people funneled into the narrow stairwell with persons at the bottom stopping to prevent falling down the stairs and the people on top pressing the crowd into a gridlock of bodies that was unable to move. The persons at the bottom did fall and became barriers for the rest of the group. This dogpile lasted for about 30 minutes with first responders seemingly helpless. Twenty-one people were killed in the crush.

Directional Signage

You and I see the signs every day but imagine a tourist (who has trouble finding our restrooms on a good day) finding that emergency exit at 3:00 a.m., half asleep, and fully intoxicated. There is a sign on the back of every room door in the US that has evacuation procedures and a map to the exits. Nobody knows it is there, much less reads it when they check in. Not much to be done about that, except make sure your signs are working and posted in a way that they can be seen.

Means of Egress

The way a guest enters a hotel and finds their room is carpeted, nicely lighted, and decorated with mirrors and wallpaper. The emergency exits are remarkably different because they are not used by guests normally. Because these areas appear abandoned or neglected by management, and because they are commonly used for daily “back-of-house” operations by employees, these halls and stairs tend to get cluttered with extra furniture, supplies, and a chair for smoking. I recommend cleaning out the junk, cleaning the dust, and even painting the walls to look presentable. A clean and clear egress area will discourage employees—and guests—from abusing it. Then enforce the rule that no items are to be stored there.

Make sure that the exits actually lead to an exit. Over the years, doors get painted shut, locks get stuck, lights burn out, and even remodeling leaves a mark. Someone (Security) should be inspecting these exits at least once daily.

Doors

In Commercial construction, doors are used to separate floors and transitional spaces so that fire and smoke can be contained during evacuation. Doors that are propped open are useless and could cause an emergency exit to become unusable. Patrol of the facility should also include observing, identifying, and closing doors that have been propped.

> In 2012, the cruise ship Costa Concordia struck shallow rocks off the coast of Italy. As the ship began to flood and list, the generator was drowned, and power went out. Passengers, most of which had not been included in the lifeboat drill, were told it was just a power problem and ordered to their rooms. Of the numerous procedural problems with the evacuation, all of them could have been prevented.
>
> Those that died were generally the ones who followed the orders to report to their rooms. Those that took it upon themselves to abandon ship, found it difficult to launch lifeboats. Because the ship was listing about 45 degrees at that point, the starboard side was in the water and the port side was tilted so far that the boats could not be lowered. The starboard side was manned by employees who knew nothing about launching boats. They found ropes for the pulleys had been painted over for years and were stuck to the hull. It took over six hours to evacuate survivors, some of whom swam to shore. The captain had his own issues and was later sentenced to 16 years in prison for his negligence.

Alarm Function

Your fire alarm is inspected and maintained by professionals and are almost idiot-proof. You are given some limited control of the alarm on purpose. If you do have some control of the alarm, do not be the weak link that causes risk or loss of life. In the cruise ship story adjacent to this one, the captain was the sole person who failed to sound alarms and even abandoned the ship before everyone else. Fire alarms have different detection points depending on the location. Sprinkler heads with heat activated switches, smoke detectors (ion particle sensors), heat detectors, and even manual pull stations comprise nearly all points in a hotel. You may be surprised to know that malfunctions are quite rare. Just because there is no fire when the alarm sounds, does not mean we have a bad system. Water flow can be caused by a broken sprinkler head—where water is actually flowing. Smoke alarms can be activated by bugs, cigarettes, and human tampering. The manual pull is so fraught with abuse that many jurisdictions no longer use them. Of course, each of these components can have a malfunction, but it is usually caused by a human.

False Alarms

I tend to avoid the use of the term “False Alarm” with guests and employees. It creates a feeling of complacency to the point where the alarm is ignored. I generally tell folks that there is no fire and no cause for concern, that the alarm did what it was designed to do and we are investigating the cause. When that alarm activates, for whatever reason, it is a great time to practice response procedures. Remember earlier we discussed that the evacuation was most important. Whether it was required or not, some people will hear an alarm and evacuate. The first part of your de-brief will be to determine what egress areas were not monitored by an employee and adjust your plan accordingly. Then you will identify things that did not work correctly such as stubborn locks and door closures, elevators (which drop to ground during an alarm), and the alarm itself. Finally, it gives you a chance to work with the fire department and see what their priorities and procedures are. I have seen alarms where the employees are running around like chickens with their heads cut off while guests are descending the emergency exits, encountering lights out, tripping on obstacles, getting lost in the maze of hallways, then forced out into inclement weather while the employees are oblivious.

Bottom Line

Your fire alarm response should make a safe evacuation its primary objective. Deploy employees to the Fire Command Center or to where the Fire department arrives to provide communication and support. Send one person to the point of detection to evaluate the situation and radio back to the Firefighters so they know what equipment they will need. All hands on deck should be assigned to emergency exits to escort guests safely out of the building. Even if you determine it is a false alarm, those in the fire stairs do not know that and need to have some communication.

Fire

A small fire in a trash can, depending on its location, is likely not to set off any alarm until it is too big to handle. If you are alerted to this fire in the early stages, resources should be sent to it to attempt extinguishment and to evacuate the immediate area. Call the fire department early and then call them again when you have more information. Someone meets them and then communicates their directions to the team.

In 1980, a fire engulfed parts of the MGM Grand Hotel in Las Vegas, NV. It started as a short in the wiring of a refrigerator in one of the restaurants. The fire moved very quickly (15 feet per second) across the casino, killing 18 gamblers. Others were killed being consumed by smoke in the lobby, elevators, and upper floors. People breaking out their windows to get ventilation allowed black smoke outside to come inside the building. Over 1,000 people were rescued by helicopter off the roof and a total of 85 people died.

This was a calamity of errors—as most human-caused disasters are: Many violations documented by inspectors over 5 months prior to the fire had not been fixed and many other recommendations had not been followed, either. There were no sprinklers in the casino, the elevators had no fire safety switches, and the count room had better protection than any place in the building.

Three months after this incident, another fire broke out at another resort, killing eight people. Major code changes were made after that one.

When Nevada passed its indoor clean air act (no smoking), it was missing a few things. One was ashtrays in No Smoking areas. What is the big deal? Well, we being the obedient hotel removed all of the ash trays from elevator lobbies as instructed and then nobody could put out their cigarettes before boarding the elevator. Not only did this create a fire hazard and confusion for the guests, but we ended up with hundreds of burns in the carpet where cigarettes were snuffed out. Another thing missing from the law, besides common sense, was an enforcement arm. In other words, though smoking was illegal in certain places, nobody could write you a ticket, take you to jail, impound your cigarettes, or look at you funny. Once I realized this, I put all those ash trays back in the hallways. Better to ask forgiveness than permission, except I did not even need to do that. There were other flaws in the law, like smoking was still permitted in casinos, which has got to be about 90% of the smoking in the state. I forgot the point of my story, but it is important to consider that there are fire hazards everywhere among us, even those disguised as laws.

Active Shooter

The term conjures up images of mayhem and horror for most people and so it should. The homicidal maniac is one of the deadliest, most unpreventable situations we will face in our industry and has been declared in several surveys to be the threat that keeps Security Managers up at night. I used the phrase "Most Unpreventable" because some shootings are preventable, unlike hurricanes and volcanoes which are not. I use the term "Active Shooter" to denote any type of shooting or assault with a deadly weapon. Someone swinging an axe or wielding a knife can be just as dangerous. In fact, most European countries have just as many incidents as we do, but they are usually with sharp instruments as guns are not as readily available.

The only ways we have to prevent these rampages are: Awareness, target hardening, and communication. (My, that term comes up a lot, doesn't it?) Notice the following plan corresponds with the section on workplace violence in Chapter 11. Our plan derives from knowing a little about the shooter and looking at past incidents, their techniques, their targets, and their motivation.

There are four types of shooter and OSHA has diligently classified them into different types. (All shooting incidents are "workplace violence" unless it happens in the home or away from any business.)

The first type is the unknown shooter. He can be a robber, gangster, terrorist, or anyone that is a stranger to the business. His intentions are criminal and rarely random. If he targets a hotel, it is usually because he has a connection to it.

This is the hardest shooting to prevent because we do not know the suspect nor the time he will strike. Strong physical security measures are the way to prevent these shootings. Behavioral Recognition, metal detectors, and other physical and electronic barriers are what we use to prevent these acts of violence. When doing a risk assessment, you will likely place Active Shooter high in both severity and likelihood.

The second type is a business, student, or patient relationship. This person is known to the business (as a customer, not an employee) and likely has a grudge against someone or something within the business. The shooter on October 1 in Las Vegas was of this type because he was known to the hotel.

If you knew a disgruntled guest was going to come back with a firearm and start shooting, would you have treated him differently? In most cases, the answer is yes. This exemplifies the need for great customer service and going above and beyond with guest issues. This is not to say your poor customer service will lead to a shooting, but you will never know how many situations you might prevent just by being civil and even sucking it up. The guest is always right. It also highlights the need for employee awareness and communication which is detailed in Chapter 11.

Type three is the disgruntled employee. The term "going postal" was derived from this type of violent person. This is an employee or former employee who has a grievance against the company or an employee. We see this type of shooter far too often in the travel industry, yet this type of violence is the easiest to prevent.

Prevention of disgruntled employees is simple if management is paying attention. This is detailed in the section on Workplace Violence. If you look at shootings where an employee was terminated and came back to seek revenge, it was obviously always on bad terms that he left. A good HR department will not allow an employee to leave who has lost all hope and has nowhere to turn. Security can play an important role in major discipline and separation of employment. I always took it a step further and asked the HR director to let me do the term myself. I felt if I broke the hard news, it made it less personal so the employee would not have a grudge with his boss or even HR, but with me.

The fourth type of violence in the workplace is domestic. This can be a jilted lover, ex-spouse, or estranged partner. Whether the assailant is an employee or not, the targeted victim generally is. We have seen these types of assailants over and over. The spouse has a restraining order or is unable to physically attack his victim at home, so he goes to work where he knows he can find her.

The prevention would be simple if the employee/victims were all transparent in their situations. Few people are going to admit or even confess that their ex-lover wants to come to work and kill them. They lay low, hoping for the best. Unfortunately, getting involved in domestic issues may be part of your job because it affects other employees. More on this is in the Workplace Violence section.

> "We have an active shooter confirmed at our location" was the transmission heard over hundreds of police radios. Within minutes, the dispatcher reports no less than a dozen more active shooters within a three-mile radius. Police responding from all over the valley with sirens wailing are thinking about triage, taking down one shooter, assisting their dozens of brothers assigned to the first venue, and now they imagine a multi-pronged terror attack that has shooters at several major resorts. Thoughts of Mumbai and 9/11 must have run through their minds as they try to sort out the chaos.
>
> Soon, the incident commander comes across the radio and orders the dispatcher to check with each resort to see if they really have their own active shooter. As is reported less than a minute later, victims—walking wounded—are seeking shelter at other resorts and their screams and blood are being interpreted as more active shooters.
>
> Even if for only a few moments, police and residents of Las Vegas, Nevada believed they were victims of the most widespread, coordinated terror attack in history.

As for prevention and response to a shooter, in general, there are some things to be done to prevent, or at least reduce casualties. Awareness by employees is the best measure you can have. We have seen on so many occasions in the news where a visibly armed gunman walks into a lobby or reception area and no one pays attention to him unless he is already shooting. I keep coming back to the concept of the Walmart greeter. When you train your employees to look up, acknowledge and greet your guests, you are not only providing great service but also that awareness of seeing someone that does not look right. The second sense we ask employees to use at work is their hearing. Historically, when there is an active shooter in an office building, school, or warehouse, we have interviewed survivors who were in denial when they heard the shots. Having no explanation for hearing shots in their workplace, their mind tried to deny it, thinking it could have been fireworks or a backfire or something else. Of those scenarios, the gunshots are actually the most likely, yet we refuse to acknowledge that possibility. Those few seconds thinking about the cause take away from the seconds needed to survive.

Response

I have taught many classes on active shooter, and the biggest concern among students is having a documented plan. This is something the boss usually requires, but that is not the only reason. If you have a shooting at your place, your guests and employees will need some guidance. Having a plan that you exercise will save lives. Besides, if it does happen, you do not want to be answering to someone saying we showed the video. You have a duty to your guests (and employees) to do more than the minimum. Saving lives is not an optional part of your plan and neither "Run, Hide, Fight" nor "Lockdown and call 911" directly address that obligation. Remember in just about every chapter of this book, so far, our primary objective has been "Guest safety."

Of course the two responses above should be trained in advance to everyone without exception. In my opinion, we do not put enough emphasis on "running." So many studies have been done on the survivability of running away, whether you hear shooting, or are actually faced with the shooter. In fact, how often do you hear of shooting victims being shot in the back as they ran away? I have always been haunted by the scene of students cowering in the corner of a Virginia Tech classroom waiting to be shot by the gunman (see text box).

In 2007, a student entered one of the buildings of the Virginia tech University campus armed with two semi-automatic pistols and hundreds of rounds of ammunition. As he entered the Hall, he chained the doors shut and placed a note on one of them that they were booby trapped. He went to the second floor and attempted to enter several classrooms to shoot students and professors. Most of the killed and wounded were students who either did nothing or were attempting to defend themselves and others by charging at the gunman. In one classroom many students were shot who are in the corner of the room surrounded by chairs and desks. Other classrooms had heard the shots and successfully barricaded their doors. In one classroom the majority of students jumped out of the second floor windows to safety. The police were delayed in their response by the chained doors but as they reached the second floor the gunman shot himself dead.

I am not suggesting deviating what has become a national standard—Run, Hide, Fight. But I do recommend that if you do additional training, and you should, use an expert to show the options and case studies to provide more and better options to keep employees safe. It is important to note that when faced with a life-threatening situation, people, in general, will revert to muscle memory. If they have no applicable muscle memory, they will revert to their instincts—which may be to do nothing. If all they have done is see a video, there will be some valuable seconds lost as they process the memory of the video and decide what to do.

For all of these reasons, there should be some physical training on what to do. By physical, I do not mean going to the gym. This is a simple walk-through of their evacuation routes. A five-minute exercise of hearing shots or screams or whatever and immediately heading for the nearest exit—or the one farthest from the threat—will put that action into everyone's muscle memory. (This type of training is discussed more in Chapter 3). The number of dead who heard the shots and remained in denial until it was too late can be researched more. "Probably fireworks," "Sounds like a car backfiring," "How could there be gunshots when we have locked doors?" We have all done it and it is almost always a false alarm. Plus, we do not want to look like an idiot because someone is playing a prank. That is a personal decision, I suppose, but I can tell you that people with prior training or exposure (such as military veterans) are more likely to survive because when they hear a bang, they are out of there.

Employees should be trained and exposed to the possibility for threats. In a hotel, they will be expected to assist guests during an emergency, but telling them what that assistance looks like, is your responsibility.

Security Response

As I mentioned before, we cannot have security officers—and even responsible managers—running away from the building when we have guests and employees inside during any event, but certainly an active shooter. This is the plan I expect you to have, your lawyers and risk expect you to have, and your guests assume you have.

> Elsewhere in this book I told you a story of the police chasing a gunman into the building finally shooting him near the elevators. And now the rest of the story. We had a security officer assigned to watch those elevators, checking room keys of all guests. He was posted there and knew nothing about the gunman until the police came up with his gun out and standing by the elevator. Like a good security officer, he thought he should let everyone else know about the impending danger. Rather than using his radio as he was running away from the scene, he used the house phone that was right next to his podium, stretching the cord as far away as possible while the police officer had an indignant look of "get out of here" on his face. After the event was over, we viewed the video and laughed hysterically. This is a great example of muscle memory. When in an excited state, most people will revert to their habits over any written instructions, or even verbal orders they are given. This officer had used that phone several times a day for years to talk to his dispatcher.

Please scale these procedures based on your staffing levels and size of your facility.

Objective

Direct guests and employees to safety, tend to wounded, and support police response. Note that the objective is not to apprehend or foil the shooter. The police will take care of that. We are not trained, equipped, or expected to take on an armed person. Our objective is always guest safety, which includes evacuation and/or assisting injured. Other actions will be secondary.

Physical Response

As is reasonably safe, someone needs to locate the shooter and radio that location in real time to a dispatcher or someone who can call police.

All employees, as they evacuate the scene, should take guests with them, being careful not to endanger themselves.

Security officers should direct the evacuation, keeping guests from fleeing toward danger, without endangering themselves.

Personnel should be assigned to every perimeter door to keep guests from entering or re-entering (always keeping personal safety in mind).

Police Notification

One pre-designated person will call 911 (preferably from a landline). This can be a dispatcher, operator, or a camera observer.

Caller will give the location, identify themselves and say, "I have eyes on the shooter." During a shooting, many people will use their cell phones to call 911. This overwhelms 911 operators, placing calls on hold or disconnecting, saying, we know already. Your representative will be moved to the top of the ladder when they know you are with the property and can direct them to the shooter. Direct responding officers to an entry that is farthest from shooter or opposite his direction of travel. Police have to form up and enter a building tactically. They will not stroll through your lobby looking on the way to the meeting rooms. The closest, safest entry point will save lots of time in clearing rooms that you know are safe.

Direct one security officer or manager to meet the police at a designated entry. This representative will update the police with the location of the shooter and the routes to get there. The police will not take the rep with them. The rep should remain or go where directed by police. If there is a master key or other tools that will aid their mission, stand ready to give it to them.

General Procedures

Security officers or property representatives will continue evacuations, holding perimeter until relieved by police. EMS (emergency medical services) will likely be denied entry until it is safe. Assist wounded guests to the extent possible and as is safe to do so. EMS will likely set up a triage area if there are multiple casualties.

Additional Details

- Police will not tend to the wounded or do anything else until the shooting is stopped. They are laser-focused on their mission, so keep people from distracting them. They will also step over bleeding persons if they are still looking for the shooter.
- Someone needs to be designated as the property spokesperson to corral media and keep the communication controlled.
- For these plans and every emergency, make contact now with the Fire Dept and the Police Dept to verify their response and tactics. Let them tell you their preferred ingress for the variety of response types.

Here are some characteristics of active shooters that may affect your response and your actions.

- Depending on your police department, the response time can range from 3 to 6 minutes.
- About half of shootings are over before the police arrive.
- Over 75% of shooters were known to the employees (former or current coworkers, regular customers, vendors, etc.). Should you devote more resources to Workplace Violence Prevention?
- Males make up 97%.

Panic Alarm

Many of us have panic alarms installed at point-of-sale locations for employees to summon security or police in the event of a hold-up, fight, angry guest, or other violent situations. If you have these or plan on installing them, please consider the following.

1. Who will monitor the alarm? If you have a full-time security staff, I recommend that, because response time is faster, and false alarms are more easily forgiven (remember the free training that a false alarm gives you). If you have no security staff, perhaps the operator or similar person could monitor it, but then you will need to decide what they do when they receive that alarm (cameras are nice in these circumstances). If it is going to be the police, then realize that response time will be longer, and false alarms are not tolerated well.
2. Location and type of buttons. Sounds simple, but some buttons are cheap and will false occasionally. Others are too difficult to deploy when someone is drawing a weapon at you. Make sure it is mounted so that it is not hit by accident and does not require squatting and a flashlight to find it.
3. Training. Let your staff know under what circumstances they should use it. The phone is always better, so the button is supposed to be used when under duress or imminent threat of violence.
4. The phone can also be used for some emergencies. I have used a secret script for cashiers such as "I have a wet spill at the gift shop," which alerts the operator of a certain problem.

Bomb Threat

A credible bomb threat, in practical terms, is one where the suspect gives information that could be true and is specific. That type of information includes when, where, how, why, and so forth. Most threats are designed to disrupt the business through evacuations and lost revenue rather than hurt anyone. Though I suggest you notify the police, they are not going to make any drastic decisions without you, unless they deem the threat credible. Make sure your executive team has the final word on your response.

Stateline, Nevada 1980: Men disguised as photocopier delivery personnel made their way into the offices of the Harvey's Casino with a steel box about 24" x 30" x 40" (my estimate). It was filled with 1,000 pounds of dynamite. The bomber called the hotel with a threat to detonate it if the hotel failed to pay $3 million that he thought was owed to him for gambling losses.

The FBI examined the box for hours and finally decided the safest way to defeat the bomb was to use shaped charge to blow the detonator off and leave the dynamite untouched. The building was evacuated, and the charge detonated remotely. This explosion set off more dynamite that was located in the detonator as a tamper device. This ignited the large cache of dynamite and the explosion. The hotel suffered major damage but due to the evacuation, no one was injured.

1. Make sure whomever has the pleasure of answering phones at your place is trained and equipped to answer these types of calls. Search the Internet for "DHS Bomb Threat Checklist" and you will find the materials you need.

2. Once someone in charge is made aware, they will decide if police are called and whether there will be an evacuation and a search. If you are evacuating, you are calling the police.
3. If evacuating, it is best to do by word of mouth. The fire alarm and Public Address system are generally ignored, but some will panic, and you want this controlled and to an area of your choosing.
4. A search can be done in a short time, checking public and common areas such as restrooms. Look for anything that does not belong, including inside all trash cans. The outside should also be closely checked as some bombers may want to target first responders or persons evacuating.
5. Radios, especially newer ones at higher frequencies, can be mistaken for a detonation signal so their use should be prohibited during the search.
6. Other departments such as Facilities and Housekeeping can assist with search. They know their respective areas and will more quickly notice something out of place.
7. Check with your Fire Dept and Police to see if they have certain protocols they want followed.

Medical

I bet medical calls are the most common emergency at any hotel. Accidents or illnesses are responded to in the same manner.

1. Make sure your call-taker is trained to receive these calls and get all of the information from the caller. It will be up to that person to make the decision to call 911.
2. I would call 911 right away (sight unseen) if the caller says any of the following:
   a. He is not breathing
   b. She is choking
   c. I think he is having a heart attack; stroke; seizure, etc.
   d. He hit his head
   e. The bleeding is not stopping
   f. Victim of an attack of any kind
   g. If they request it, no matter the situation
   h. She is pregnant
   i. Unconscious
   j. A child
   k. Anything else that is serious or life-threatening
3. Remember to call 911 first. Waiting for an assessment from a responder can waste valuable time. You can always cancel EMS.
4. Whatever equipment that security is trained to use should be brought to every incident (defibrillator, oxygen, first aid kit, etc.). This training is covered in the next chapter.

   A hotel in Nevada wisely deployed defibrillators and trained each officer on their proper use. This program was quite successful and saved several lives. However, in one incident, caught entirely on video, a man was found unconscious in the lobby. The first officer responded in seconds but did not bring the defibrillator (AED) as trained. The second and third officers also responded very quickly and did not bring the defibrillator. The supervisor arrived, also with no AED. The officers could detect no heartbeat but heard gurgling, so they assumed the man was breathing. An ambulance was called, and paramedics were on scene eight minutes after the man went down. They immediately deployed their defibrillator, which malfunctioned.

The supervisor called for the hotel's AED and the man was revived after being shocked by the AED. The man survived but his family sued, as he did not fully recover from the brain damage. In court, the family subpoenaed video and reports from seven other incidents where the first officer to the scene brought the AED. They also showed the hotel's training program, which mandated the AED be brought to every medical call. The hotel claimed that they thought the man was just drunk and unresponsive because they heard him gurgling. As you guessed, the hotel took a serious hit because the training was not consistently applied.

In this case, the hotel had AEDs, had a policy to bring them, and violated their own policy. It was easy for the plaintiff to prove that they contributed to the man's ill health.

5. Depending on the incident and condition of the patient, perform only those first aid functions that have been trained (by the company—not in the army or elsewhere) and keep them stable until help arrives.
6. I recommend not allowing good Samaritans to intervene. Depending on people's training and experience, their view of treatment may differ from ours. Their malpractice will come back on the hotel so just thank them and keep them away. The exception to this would be a major incident when you do not have enough staff to deal with it.

Suicidal

I have seen too many suicides and concluded there are two types. One does it in the privacy of their room and it is usually not found until the room is cleaned. The other is seeking notoriety or intervention by making it very public—jumping from a garage, rooftop, or balcony; self-inflicted gunshot in the lobby; even running in front of a truck. I have seen all of these and it is a horrible event for everyone involved.

There has been a subtle change in response to these calls—at least from what I have seen. I saw a family sue the city when police tried to wrestle a guy off a ledge, and he managed to jump anyway. Apparently if you intervene or encourage them it will be your fault. So I recommend checking with your legal folks to see what they want trained. Meanwhile:

1. Keep the area clear of bystanders. Other people will mock, get in the way, try to intervene, or take video that will be used against you.
2. Notify police and EMS no matter what. Even if the person changes their mind, they may need some treatment.

Lost Child

I was the first one representing a hotel casino to collaborate with the National Center for Missing and Exploited Children (NCMEC) to institute "Code Adam" procedures.

In 1981, 6-year-old Adam Walsh was abducted from a Florida department store and horrifically killed and dumped in a drainage ditch. The killer was identified but never convicted due to evidence problems. He dies in prison, serving time for other crimes. His father became a staunch advocate against criminals of all types and has had at least two television shows highlighting wanted criminals.

Congress passed several laws in the past 40 years to prevent the abduction and find missing children. The NCMEC was funded initially by Congress and is active to this day in all of these issues, including stopping trafficking. In 1994, Walmart stores established a "Code Adam" procedure, where once notified of a missing child in their store, it is locked down and searched until he or she is found.

Code Adam simply mandates that when a frantic parent notifies you of their child missing, the building is locked down, so no kids enter or leave the facility until the missing one is found. Since I had a large amusement area for kids, it was natural for us to have a process. The NCMEC can assist with this program and all departments can get involved. I listed this in the "Emergency" section because time is critical in responding to a lost child.

Another lost child that happens all too frequently is the toddler that sneaks out of his room in the middle of the night while parents are sleeping. He wakes up and either seeking the bathroom or a good time, walks right out the hotel room door. Once he explores the floor and tries to come back to his room, they all look the same. Some will wait until a guest checks on the noise in the hall. I have seen others get on an elevator, making it harder to find them.

Unfortunately, death or kidnaping can result from a toddler on the loose. So I recommend locking down the hotel as in a Code Adam and calling the police. If you have an equipped door lock system, you can see what door was opened in the last X minutes.

In 1992, musician Eric Clapton lost his son to a fall from a hotel window. In 2020, a toddler who escaped from his third-floor motel room went into the hall where he found an open window. He climbed out and fell to the concrete where he was severely injured. Please consider all possibilities when making your hotel safe as no one would want to experience what these parents must have gone through.

Notify the police immediately. Especially because you do not know how long the child was gone. They will likely do a room-to-room search.

Make sure the hotel is locked down as in a Code Adam. Have someone search that locked area in all the hiding places and make sure windows, trash chutes, and other hazards are mitigated.

Weather—Blizzards, Hurricanes, Rain/Flood, Winds

Depending on your climate, you probably know how better to handle a hurricane, blizzard, or whatever frequents your neighborhood. Contact your local County Emergency manager for advice and resources on response and preparation plans as well as recovery.

Being a hotel, your local authorities may have their eye on you to help out in the event of a disaster. There is nothing but positive reasons for doing this. Depending on the disaster, you may even be reimbursed for providing aid. I was the first on the list of available shelters in my region when we had two mass casualty incidents within ten miles.

Though all of the hotels helped out, I got to host the coroners and investigators that were flown in to help. We also made boxed lunches for wildland firefighters when needed.

Do not spread your hotel too thin as you may not have a full staff, depending on the disaster and where it is located.

Earthquake

I do not think there are any hotels left in the US that were built before earthquake codes were upgraded in the 1970s. Those that were should have been upgraded and retrofitted by now. That means, generally, it is safer in a hotel than outside if an earthquake hits. Let's go through some of the procedures.

1. Advise guests and employees to remain where they are, seeking cover from any furniture or doorways that they can.
2. Do not evacuate unless told to do so by authorities. Falling debris outside is more dangerous than inside.
3. Inspect the building and utilities to make sure there is no critical damage.
4. Prepare to receive others seeking shelter.

Power Failure

This is not a life and death emergency generally, but you need to be prepared to keep guests safe and comfortable in a power failure. Trips and falls and other injuries could be your fault if lighting is a factor. It is an inexpensive investment to have battery-powered lights ready for a failure. Make sure these devices are inspected periodically to ensure they will work when needed.

Indoor Contaminant Release

An indoor release includes everything from a gas leak to a poison aerosol.

If unsure of the nature of a chemical or its source, the building should be evacuated. Remember to always evacuate downwind and uphill. If you can smell a chemical, the cloud is already upon you.

In 2019, a college dormitory had a gas leak in the basement. The multi-story dwelling was mostly unoccupied because school was on break. A lone mechanic investigating the leak found the basement air so toxic he called the fire department. As the fire department responded in their turnout gear, they too smelled the fumes from outside the building and decided to back-off and assume hazmat gear and special breathing apparatus before entering the basement. Fortunately, as they returned to their fire truck, the gas cylinder beneath the building exploded and the lower three floors of the structure collapsed (pancaked). The adjacent building also had its entire façade destroyed on all 12 floors.

A bad valve on the cylinder had released gas into the confined space where it concentrated and then ignited from a pilot light on the other side of the basement. No one was killed because the buildings were empty. Had the buildings been occupied, the fire department would have likely evacuated the occupants upon their arrival. The casualties would have been numerous.

Outside Chemical Release

It is not far-fetched to expect a gas cloud to threaten your property from outside. Chemical facilities, train tracks, or an interstate nearby can put the property at high risk. Even construction of a new hotel or work being done in the street can cause a natural gas leak if a pipe is broken. That is considered a significant hazardous material release by the fire department and the building should be entirely evacuated.

Any type of chemical exposure, whether airborne, liquid, or solid should be treated similarly.

Evacuate the area. Airborne substances are heavier than air, even if they are invisible. This means they will travel with wind or air currents but will seek the lowest point.

Do not touch objects or infected persons. Perform first aid only if risk of exposure is absent.

Notify EMS and Fire departments. Advise on safe entry point for first responders.

Locate Material Safety Data Sheets and follow first aid instructions.

Keep others away from area to avoid further contamination.

Treat location as a crime scene unless it is a confirmed accident.

I am sure you can think of, or have experienced, other emergencies in your area that are not outlined here. Please do not neglect those and outline them the same way we did here. Whatever size staff you have to work with, consider “deputizing” other team members to be activated in certain emergencies. Any employee can knock on doors in an evacuation or search for a suspicious device or assist guests in moving to another location. Always remember the objective of every emergency response is life safety.

SECONDARY EFFECTS

I learned over the course of a few decades that in addition to an initial response to an emergency there are other things (collateral damage if you will) that happen at that scene but also nearby, perhaps at other properties. My hotels were victims of both, and I will share those lessons learned as we go, but a good example is the following.

October 1, Las Vegas Mass Casualty Incident

Just as the shooting stopped on October 1, incident response was in full swing, as was the panic to evacuate the area. Thousands of people ran north and south on Las Vegas Boulevard, not knowing where to go or what to do. First responders were ignoring the walking and running wounded because they knew there were worse injuries ahead. Hotels north of the venue, of which there are dozens, were caught by surprise when hundreds of people started flooding into their doors seeking safety and shelter.

Imagine working a relatively slow swing shift on a Sunday night. The restaurants are closing down, most people have gone to their rooms, and the shift is almost over when what appears to be a riot comes at your main entry doors. You do not know why they are running, what they are running from, or if the danger is with them, behind them, or it is them. You gather your security team and head for those doors because your procedures dictate that if an active shooter is outside, you have to search those coming in. The people piling in the doors with faces of shock and fright were not having that and the order was given to just let them in.

Once inside, it was discovered that they were running from a shooter in an unknown location firing hundreds of rounds. He could even be coming this way. Time to activate a major emergency protocol, which every Vegas property has and exercises.

- Police were called but were of little help because they were overwhelmed and did not really know what was happening either. Then came the call to shelter-in-place.
- The mass notification system for the hotel activated but had trouble reaching most of management because they had already gone to bed with their phones off.
- Those that were contacted, including the director of security took almost two hours to get through roadblocks and gridlock and chaos on freeway and streets.
- We have a bunch of people to feed so let’s set up some banquet rooms and get it on.
- Oh, wait, restaurants are closed and chefs have gone home. We have an employee dining room, but they make just enough for the scheduled staff.
- This hotel and dozens of others called police to report persons with blood and serious injuries coming in their doors and the police interpreted these calls as additional active shooters at those respective properties. (I was listening to the scanner and I, too, thought it was a coordinated multi-pronged attack on the strip.)
- Hours later as food was being scraped together and more management showed up to help, it was apparent that the police-ordered lockdown was going to last for a while.
- Sheltered guests began raising concerns about their medications, their pets at home, the babysitter, and numerous other things that nobody could really help with.

Some other lessons learned from this incident and others:

- Keep advanced medical supplies on hand like tourniquets, and enough for many victims.
- Make sure you have a PA that reaches the entire facility to update guests and victims. Fire Command may work for this.
- Keep a payroll list to do an employee headcount.
- Paper rooming list that includes handicap guests.
- For when restaurant is closed, consider some sort of MRE (Meal Ready-to-Eat) or other packaged nutrition. Keep plenty of bottled water.
- Force executives and key employees to keep their phone on even when sleeping and to keep their radios with them.
- Keep a scanner on hand to listen to police updates. There are apps for this on your phone.

- If you do not already have a teleconference account or conference call account, get one.
- Set up mutual aid agreements with neighboring properties in advance—though they would not have worked in the Las Vegas incident.

The only good things that come from these events are the lessons we learn for next time. There will be a next time, and possibly one that you did not foresee. Rather than prepare for every possible contingency, it is best to prepare for the certain responses that we will have to those events. It is much easier to plan for a fire alarm, for example, rather than all of the places where a fire might start.

As for the secondary effects, take some lessons from above and instead of imagining that you will have thousands of shots fired across the street, plan for having a shelter-in-place event where you house people for hours and even days. On these incidents, always remember and never forget, you must have an objective—or several—before you write a policy, procedure, class, or course. Teaching people how to react during a fire alarm, can go many ways unless you tell them the objective is to safely evacuate our guests. (Or maybe it is not. It is your class.) To illustrate my point, there was a fire alarm in the kitchen area at a large hotel where I worked. As it is supposed to work, the adjacent areas hear the alarm also so that everyone that could possibly be affected is aware of the danger. The kitchen crew had been instructed to evacuate when they hear the alarm, and they did. Unfortunately, when I got there, guests were walking around minding their own business–the alarm sounding overhead—while the employees were all outside. No one had ever told them what to do so they reverted back to first grade—when you hear the alarm, go outside.

I suggest to you that you have the following as one of your objectives—and it should be first and foremost. "Make sure guests are safe,"—simple as that. Fire alarm, active shooter, earthquake…make sure guests are safe. Of course, we will add that no one gets to run into a burning room or take a bullet. I am talking about taking guests with you when evacuating, assisting the injured instead of stepping over them, and so forth.

Recovery

I am going to gloss over this because to do it right, it would be an entire book on its own; in fact there are some great books out there already. It is an important topic and if you do not have a plan, you need to work on this right away. Most businesses that are affected by major disaster (fire, shooter, hurricane, etc.) do not recover. They do not recover. After hurricane Katrina, most hotels were condemned or went out of business after a day or months of trying. The ones that survived were supported by their corporate parents. Besides the human toll and the damage, employees get laid off, lose their insurance, and the community is decimated.

I have a quick solution that I have introduced to several hotels and I think it works well if it is given some effort. In my opinion, a plan for every contingency is very extensive and when stuff happens it is mostly unused, sitting there on your top shelf. Having been through some major crises, I found that decisions and remedies are fluid and on the spot. More important is the communication and collaboration during the event. Here are the steps to my plan, which is surprisingly simple.

1. Your Crisis Management Team is really the same as your executive team: Hotel manager, Restaurant manager, Security, Facilities, etc. You do not need a separate team because these guys will be involved anyway. If they want to delegate their participation to someone, fine.
2. As we learned at the hotel above on October 1, 2017, communication is vital. Find a way to either get your team to the hotel within minutes or on a conference call immediately.
3. Once the crisis is stable, set up a meeting of the team.
4. The team leader, presumably the GM or you, gathers information from each department. This is a current situation report. (Sitrep for you military folks.) The leader sends the Team to gather information: What is broken, what is open, what do we need to do to clean, to repair for open, supplies, food, etc.
5. Second meeting: The team reports back, at leader's direction, formulates objective. Open for business, partial business, close and start over, close permanently, etc.
6. The team prioritizes task to reach above objective. Estimate of cost and time.
7. Leader assigns tasks. Marketing establishes website, HR sets up temporary benefits and payroll station, Security sets up fire watch, etc.
8. Depending on nature of disaster, regular meetings until finished.

I call this the collaborative method of recovery but it needs structure or it will be chaotic, unorganized, stressful, and ineffective.

As long as you plan for this event, before it happens, you will be on a better road to recovery. An important part of your pre-planning is networking with regional directors, chiefs, first responders, county, and city department heads, etc. I will go over that in Chapter 9.

Mutual Aid

The term "Mutual Aid" is a few hundred years old, but I think we know it from our local police and fire departments. When there is a disaster in one city, it is common to see an adjacent city send resources and manpower to assist. The finances get worked out later. It is also common, at least in government, to have a "Memorandum of Understanding." This is generally between two agencies or perhaps between an agency and a private business. This is not charity, usually, but an emergency transaction for which costs are billed back later, according to the memo.

I recommend having a relationship with other hotels, food suppliers, gasoline for generators, bus companies, and anything else you need that you cannot store yourself. Most businesses welcome this opportunity to trade services, especially with a hotel that can provide lodging, food, and other services for their employees and clients.

INCIDENT RESPONSE

One of the functions of the security department, after ensuring guest safety, is to document and investigate incidents that may become claims. This is a customer service function as well as a way for us to protect our assets. As we transition from life safety to less harmful events, we will also transition to the investigation and risk avoidance. First, we will review some types of incidents and security's reaction to them, and in the following pages we will see how we investigate them. Nightclubs, which have their own issues, are covered in Chapter 10.

Medical Incidents

EMTs on staff—Rural properties may find it necessary to have medically trained personnel because ambulance response is extended. Before making this decision, I would weigh the risks and rewards. Of course, it seems like a no-brainer to have an EMT respond to a sick guest for better and faster care. However, look at the probable medical situations you are going to have and decide if an EMT makes those any better. For example, a heart attack would likely be treated with CPR and a defibrillator. An EMT adds nothing to those procedures. The only thing an EMT might be able to do differently is to administer drugs under a doctor's supervision. (These laws vary by state.) Even if you could do that legally, are you willing to take on the responsibility of securing narcotics and other potent drugs on your property for that purpose?

My recommendation would be to train your entire staff on first aid, CPR, and use of AEDs (Automatic External Defibrillators). This type of care has gotten so advanced, yet simple for the layperson to administer that it beats just about anything an EMT could do. If you do have EMTs, I would urge you to have a tight leash on them. It is human nature for medically trained personnel to want to diagnose symptoms and to put their patients at ease. Years ago, in a Las Vegas casino, a security EMT responded to a gentleman who was feeling light-headed with a headache. Everything the EMT could check seemed normal, so he recommended the man go to his hotel room, take some Tylenol, and sleep it off. The man died in his sleep later that night.

911—Some hotels transfer anyone that dials 911 to the hotel operator or the security dispatcher so they can get a faster response. This probably works out most of the time, but you cannot ignore the training a 911 operator receives to deal with the myriad of medical situations they encounter. You cannot afford to train your staff to answer those calls. Better yet, let the calls go to the 911 center, but arrange with them to notify you of problems in your hotel.

Whatever the training of your staff, you have an obligation to your guests to get them the fastest and best care available. Your personnel may be fastest, but they are not best so remember that they are a supplement to whatever your state, county, or city provides. Stay away from diagnoses, advanced medical care, and underestimating health symptoms. In fact, do not use your quick response to delay care. If someone calls from a room with a head injury, critical illness, major bleeding, or other life-threatening condition, call EMS right away. Waiting until your officers get to the room and evaluate, costs precious minutes.

Domestic Fights

It makes sense that couples who are prone to fighting will do so on vacation—at your hotel. Please note that you are not obligated to make arrests, take a report, provide counseling, or resolve the argument. Your obligation is to the safety of all of your guests. Some cities require the police to do certain things, but not the hotel. It may be tempting to separate and interview the parties, make special arrangements, and allow them a continued opportunity to disrupt your business. A better choice is to disconnect yourself from the emotions and salvage the night for all who were affected.

At the first sign of a disturbance, make contact with the room. We do not need a reason for the argument. Make sure neither party is injured. Does either party want the police? Because if we have to come up here again, we will be calling the police. One warning, then eviction. Do not feel like you must help with reconciliation. This is a hotel with hundreds of guests and these people are hindering your ability to keep your other guests comfortable. Arguments or physical fights are an emotional situation, even for the hotel employees who may get in the middle of it. My recommendation is to keep employees out of it. A verbal argument in a room is not good for the hotel business. You do not have the power to stop two grown adults from hurting themselves. You do have the power to stop them from ruining everyone else's night. I recommend that on the first sign of a disruptive argument, you make contact and issue one—and only one warning. Be ready to enforce your threat and evict the guests upon the next violation.

Suspicious Person

This is a broad category and the foundation for what we do. Security needs to know everyone who enters the property and should be trained to do so. That does not mean we interview every individual, but if we "know" everyone we encounter, then it enhances the guest's perception of our guest service and reduces problems.

There are a few techniques to knowing your guests. There is the greeter who stands at a door, greeting each person that enters, while doing some behavioral analysis. This can be done while on the move as well. If you have heard of the rule that requires a smile when so many feet from a guest and a greeting for shorter distances, then that is another method of identifying suspicious persons.

Security officers know who belongs and who does not. If he/she does not, then you have to train him/her to recognize persons out of place and unusual behavior. This is not rocket science or profiling. Well, it is profiling, but not racial or any other type of discrimination. It should be very simple to look at a person's dress, their actions, and even their hygiene, and decide if they need a second look. The easiest way to avoid errors in judgment and allegations of discrimination is to train every officer to greet every person they see.

Of course this enhances your guest service, but it also forces your staff to engage in good guys and bad guys. "May I help you find something?" This is especially useful in the hotel where anyone encountered should be a hotel guest. "May I help you find your room?" The end game here is to let every would-be criminal know that they will not be invisible on your property.

Trespass

I have said throughout this book that we are not law enforcement officers and it is rarely in our interest to make arrests. In most cases, it is better for all involved to simply get the person off property. In most states, the trespassing law is a tool that private property owners can use for just that purpose. Other crimes, such as larceny, battery, and vandalism have to be proven for you to make an arrest. Rather than spending time and resources trying to justify an arrest, we simply kick the offender off property, trespassing him/her in the process.

Trespassing someone constitutes (in most states—check with your local police) ordering them to leave, telling them they cannot return, and warning them of the consequences if they do. Once given that warning and they refuse, they are subject to arrest. Depending on policies and training, you either make the arrest or call the police. Some businesses call the police to give the trespass warning but that is not a requirement.

In Hospitality, we use the term 86ed to mean "ejected, kicked out, or trespassed." This term has an enigmatic origin with many theories as to where it started. In the restaurant industry, it dates to the 1930s when an item was out of stock or removed from the menu it would be placed on the "86" list. But that does not explain why the list is called 86.

A bar in New York called Chumley's place operated in the 1920s during the prohibition. It had two entrances: 86 Bedford and the courtyard in the back. When the police would do a raid, they would call ahead as a courtesy and tell them to send the drunks out the 86 entrance to avoid any problems as they were coming in through the courtyard.

The last stop on the Chicago L train was the 86th Street Station (it is not the last stop anymore) years ago and it was procedure to remove all the drunks and transients from the train before it went out of service.

One other legend refers to the soda jerks of yesterday who used numbers for just about everything. "86" meant "all out of it."

One more legend refers to the "old west" when Whiskey was not as strong as it is today (maybe 30 proof). So when they wanted to get rid of someone they would give him the 86 proof—presumably to knock him out. Seems like the hard way to me.

I use Trespassing for everything. Here are some examples.

Your cocktail server reports her boyfriend is on property in violation of a restraining order. You can and should call the police, but you can also give him a trespass warning. You cannot make a citizen's arrest for a restraining order violation, but you can for trespassing, so it gives you some options if he starts to get threatening—or worse. (I used the term Restraining Order to include any court order that is meant to keep someone away from your employee or your business. It may have other names like Protection Order.)

It is best not to get involved with the dispute itself. These orders are issued by a judge who has only heard one side of the story, in most cases, so the guy may not be the problem. However innocent he is, he is still violating the order and she is your employee, so assist her with the enforcement by calling the police and then stay out of it.

See Corporate Restraining Orders in Chapter 8.

You find a man cruising around your hotel floors. The first time, he says he is lost and leaves the area. An hour later, you find him on another floor. A quick check shows he is not a guest and is not visiting a guest. He has not broken any law so far, but you can trespass him. Next time you see him, he will be committing a crime—trespassing.

A similar situation finds two men walking in your garage, in between cars. No burglaries have occurred yet and when asked, they say they are just walking through as a shortcut home. Trespass them right away. Next time you will not have to wait for a crime to occur.

You have a drunk at your bar refusing to leave and causing a disturbance. You can trespass him and then if he still refuses, you can forcibly remove him from the bar (trespass arrest) instead of waiting for the police.

An employee gets caught putting donuts in her purse. She goes to HR and is terminated. She should be trespassed because she is a thief and we do not want her on property. Any one arrested should be trespassed as well.

A woman identifies a man whom she thinks stole her purse. He was the only one in the area when it came up missing. You have no authority to hold him or arrest him, but you can trespass him. Detaining him long enough to get his ID and "horsepower" and trespass him is reasonable and acceptable. If he refuses to cooperate, you cannot physically hold someone or surround him to get his ID. Let him go, trespassing him along the way. You can then pass on his information to the police, who may or may not investigate. When I first started in the business, we would bring the guy down to the office "voluntarily" to await the police so they can get this "cleared up." There is nothing voluntary about security officers in uniform "asking" someone to come to the office and wait for the police.

Room Losses

Guests may report missing items from their room, usually blaming the housekeeper. This, like most calls, is the beginning of a "preliminary Investigation." The information obtained will be used by Investigations to provide facts to Risk or Claims or Guest Services—whatever you call it.

It is important to gather all information, but even more important is the officer's demeanor with the guest. He or she should avoid saying things like "Oh this always happens. You will find it in your luggage when you get home" or "We had a housekeeper once who stole a diamond ring. Can you imagine?" or "I hope I can get this done today. I go home at noon." The guest's vacation is likely ruined, they are angry, frustrated, and want your complete attention to their missing item. The interaction should take about 20 minutes and should go like this:

> Hello, I am officer Smith. I understand you are missing something from your room?
> Yes. The maid stole my iPad from the bed.
> I am so sorry to hear that. Let me gather some information from you so we can do a complete investigation. Can you use the Find my iPad?
> I tried but it shows last location at my house before we left.
> OK make sure you put an alert so if it gets turned on or used, it will notify you.

(I am not going to write out the entire script, but you get the idea) Empathetic and to the point. Other information we need to get at this time is.

Where did you last see it? When did you last see it?

When did you last see it?

When did you leave the room and when did you come back?

Who else is staying in the room?

Value of Item

"I know you already did this, but do you mind if we check your luggage again?"

Once the information is obtained, take pictures of room and location of item.

Get a lock report. (Presumably your lock system can do this, see Chapter 12.)

Depending on your investigations policy, do not interview the housekeeper. Obtain name of the one or two that were in the room during the time frame of the loss.

As discreetly as possible, check the door to see if it closes by itself. This is a controversial issue in hotels. Of course, check your Lost and Found, if you have one.

Crimes in Rooms

If you have a legitimate crime in a room such as a broken door latch, the procedure is basically the same, gathering suspect information as well. Have police do a report and mimic their questions to get the right information.

Proprietary Loss/Damage

Theft or damage to company property is going to come down to your business policy. If the guest is present, it is fairly simple to get reimbursement on the spot. Calling the police is only useful if there is a crime—meaning intent—or if it happened while committing another crime—battery, for example.

If the guest has departed and there is evidence of a crime, it may be good to do a police report. This is unlikely to get your money back, but at least it will document the incident, especially if the suspects were related to some other crime or wanted for something else.

Once again, your business needs to decide how useful a report on these incidents is. A report is useless and takes more time than the value of the item in many cases. There will not be a police report in most cases, and you are not going to collect from their credit card. In my experience, the card on file is either maxed out, or if you do get a charge to go through, the guest will dispute it. The credit card company has little time or motivation to investigate so they reverse it. Trying to fight the credit card company on this is futile because they will say you cannot prove the guest did it and you cannot charge their card without their signature.

I believe it comes down to the cost of doing business. Perhaps you have a threshold that triggers an investigation. Most front desk systems will allow you to flag the name so if he comes back you can either refuse his business or have a talk with him about the $10 framed artwork that you are charging $150. Besides, you do not investigate missing towels, right?

I talk about trick rolls (prostitutes stealing from a guest) in Chapter 11.

Room Disturbance

I pool just about everything that happens in a room in the disturbance pile. Whatever they are doing in there, if it annoys or affects other guest rooms, that is a disturbance. Marijuana is at the top of my list but there are noise complaints, fights, parties, and much more. The response is about the same.

Let us first agree what behavior is tolerated and what is not. Get your manager and work this out in advance. Many hotels publish these rules and present them when you check in. This contract of sorts helps you with the guest, provides a first warning, justifies additional credit card charges, and notifies all guests of the rules. If you use this method, I recommend a No Tolerance policy. Otherwise, you give one warning and that is it.

I recommend following up with your warning. Your reporting party will get really frustrated if you go up, warn the occupant, and the noise starts up after you leave. Do this yourself about 15–30 minutes after you leave to make sure your warning has been heeded.

Bed Bugs

Bed bugs not only make the occasional appearance in hotel rooms, but also, they have infested news reports and blogs. Although no one has come out and reported an epidemic or widespread infestation, the perception is clear. Sometimes in the tourism business, perception is more important than reality. And the perception now seems to be that it is a big problem. One recently published list of the 15 worst cities for bed bugs seemed directly proportional to population, with New York at the top, so it is difficult to see any trends.

Provided here are some facts about bed bugs that do not come from the people paid to eradicate them or from the agencies that spread the news. I hope that you will be able to use this reality at your facility to change the perception and deal with this issue.

Bed bugs are tiny flat insects that resemble a small version of a cockroach. They feed on the blood of mammals. They do not fly but tend to travel on humans and in their luggage. Their small, flat shape allows them to crawl into mattresses and crevices so that they are virtually invisible until they come out to feed. They gorge on humans much like a mosquito, digging their elongated beak into the skin, and drawing blood for as long as 10 minutes. The "bite" is usually not felt and occurs at night when they prefer to come out of hiding. Although they draw blood, they are not known for carrying disease.

The insects are usually found in and around mattresses and are distinguished by their small dots of brown excrement or reddish blood smears. They do not have nests or colonies but will congregate in those dark places near their feed. Due to their size and hiding places, they are best discovered by a trained professional.

Bed bugs have been around for centuries and were almost completely eradicated in the early 1950s with the use of DDT. This did not apply to other parts of the world where they have continued to breed. The resurgence may be due to world travel. Bed bugs spread just like a virus by piggybacking onto a traveler or his luggage. They can be found in hotels, airplanes, and other tourist locations. However, bed bugs also are prevalent in households and, unlike cockroaches that are attracted to filth, they just want blood, so they can be found in the cleanest of environments. We used to assume they came in with homeless, dirty workers, rodeos, and so forth. We found that it was more likely business travelers who visit more hotels and have more exposure to a variety of environments.

Many hotels now train their cleaning staff to look in likely places for the critters. Some higher end hotels have comprehensive response programs that include cleaning guests' clothes, finding them alternate sleeping arrangements, and so forth. A few bold hotels, finding no responsibility for the actions of these third parties now treat bed bug complaints like an illness and offer the guest a trip to the hospital and little else. Prevention of bed bugs is almost impossible, but the best method is finding them and destroying them before they move on. Once again, a professional exterminator who knows where to look and how to destroy them does this. Besides poison, bed bugs can be killed by exposure to heat over 120 degrees for at least 10 minutes. Clothes can be washed in hot water or even just dried in a hot clothes dryer. Other items such as electronics that cannot be exposed to water or a dryer can be placed in a plastic bag in the sun or a hot car (if they can stand that).

Hotel managers should consult their professional pest control company before they have a bed bug complaint to devise a plan that eliminates the problem while caring for their guests. The exterminator may recommend destroying items such as mattresses and furniture that are infested as they are difficult items to treat. The hotel should make arrangements for the guests' belongings and other items to avoid spreading the problem. And don't forget that if bed bugs are in one room, they are likely in adjacent rooms. This may mean treating or inspecting as many as nine rooms (the infected room, one on each side, and the rooms immediately above and below those rooms).

Major Incidents

Periodically, you will have a major crime or accident in the room. I am talking about sexual assaults, a child falling out of the window, drug manufacturing, and just about anything imaginable. I have seen some crazy things in hotel rooms. You recall that although the police do an investigation, they are concerned with: (1) if a crime occurred and (2) who did it? We, on the other hand, need to answer many more questions like: Was there an employee involved? Was it our fault? Were we negligent? Is the guest trying to scam us, or maybe exaggerating? We do not even know most of the questions we need to ask ourselves, so our "major incident investigation" must gather all the information to be sorted out later.

> We got a report of a man climbing on the outside of our parking garage. He was going from one floor to another, with my guys trying to catch him. This went on for about 20 minutes when finally, one of my managers tried to grab him and the man fell to his death. At the time, he did not seem suicidal, but more of a lunatic. The police came and did a suicide report, but we were concerned about his family questioning that so we treated it like a major incident. That included saving all video from all cameras, tracing his footsteps back to see where he had been, gathering time sheets form every department to see who was assigned where and doing what. We also did a complete manpower analysis to show our staffing levels. Finally, we compiled a lot

of photos and got expert opinions on any hazards or other influences that could have caused this tragedy. Unfortunately, we had too many suicides from our buildings, but this was one of the unusual ones.

First, I recommend you establish a major incident procedure. It should include lock interrogations for the entire floor (yes, all of it). Retaining all of your video footage for the entire property, interview of witnesses and non-witnesses, payroll reports from employees anywhere near the crime scene.

The crime scene template will remind you of information to gather. Depending on the crime or incident, it could be a drawn-out criminal investigation and trial. If it turns into a civil case, you may not find out for months or years from today and going by memory will not work. Hopefully, you have nothing to hide and offering up evidence of that is useful.

Guest-Room Attendants

Unfortunately, we take our most vulnerable employees for granted—and they sometimes take advantage of us as well. It is your duty and obligation to maintain a workplace that is free of hazards (OSHA General Duty Clause). A lone housekeeper going from room to room can be dangerous. Housekeepers, especially those from other countries with limited language skills and no knowledge of our customs, get assaulted, intimidated, harassed, and even beaten way too much. It is often not reported—or it is downplayed to avoid scrutiny on her part.

There have been some high-profile cases about these crimes, but if you spoke to the GRAs privately and in confidence, they will tell you that men answer the door naked, make passes at them, speak to them inappropriately, truly to get them to come inside, offer them money for sex, and on and on. This is unacceptable and you should make every effort to stop it. See more information on prevention efforts in Chapter 11.

If you do get a call like this, it will be a “he said, she said.” Document the incident and make a report. Notify management and ask either one if they want to press charges. If police are not involved, you will have to investigate. Criminal acts by the guest should be reported to the police. Non-criminal acts should be turned over to management to decide if the guest should stay or go.

If the housekeeper has misbehaved, she must be suspended or dealt with immediately. Housekeeper theft in Chapter 8.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

8

Investigations

The first hotel security personnel, dating back over 100 years, were referred to as "detectives." Today, there skills are just as necessary and just as valuable. Investigators serve many purposes in modern-day Hospitality, but primarily they allow the hotel to resolve claims and prevent future incidents.

Corporate investigations are much different from police investigations. The objective of the police is to solve a crime, make an arrest, and prosecute someone for the offense. In our world, most of our investigations are not criminal at all. In most cases, we are trying to prove that the hotel is NOT to blame for an incident and to prepare a defense for a claim against us. If we are to blame, we may be enforcing policies rather than laws.

Investigators work closely with the Risk or legal department to make sure we have evidence, video, photos, and witnesses to resolve a claim. Investigations are necessary to not only prepare a defense, but also to find vulnerabilities such as weak policies, employee misconduct, or environmental conditions that we can improve to prevent the same occurrence from happening again. For example, an investigation on a guest slip and fall might reveal a porter using too much water mopping the floor, or a floor that is too smooth, or the lack of maintenance on a certain area. Or it might show that the accident was unavoidable or the guest's fault.

Some investigations will result in such actionable findings; some will go to Risk when a guest demands compensation for an incident; a small percentage of those will result in litigation; and others will be used internally for discipline, maintenance, and policy changes. Our investigations will not be used in a criminal case. That is up to the police. This makes our investigations more fruitful which we will cover shortly.

Sometimes the C-suite will decline having investigators or doing investigations because they expect the police to do that. I hope after reading this chapter, you will be able to educate them on the value of your own investigations which actually save the company money.

PRELIMINARY INVESTIGATIONS

Much of the investigator's duties involve looking into guest incidents to make sure the Risk Manager has all the information needed to process a claim or respond to litigation.

DOI: 10.4324/9781003037644-8

We, therefore, start with the preliminary investigation which begins when Security first learns of an incident.

The purpose of the preliminary investigation is to gather and document as much information as possible while the guest is still present, or while the incident is still "fresh." Also called Field Investigations, the process begins at the scene of the incident by the responding security officer. Security gets all sides of the story, speaks to witnesses, gathers statements, takes photos, and documents the incident so that it can be turned over to an investigator for more thorough review. Every incident has some sort of investigation, even if the responding officer at the scene concludes that investigation. We will start with that initial response, gather evidence, and then begin the investigation itself.

Initial Response

The investigation of any incident begins as soon as the first officer arrives on scene. The officer has already begun the process as she approaches and mentally records the scene. This recording includes what the scene entails: persons present, their actions, placement of objects, condition of the area, weather, lighting, etc. It is up to you to train the officer to memorize and document these important pieces of data. Granted, not every piece of data is relevant to every scene, but rather than try to distinguish in advance which ones are, it is better to go for the entire thing. Sorting through too much information is better than later wishing that you had it. Providing the officer with tools will allow her to do this preliminary investigation completely and efficiently.

Preparation

Training, as usual, is the first step. Start with an awareness of the goal of the investigation. Most officers do not take the time to be as detailed and thorough as they could because they do not understand the criticality of the investigation. It must be explained to them that even though maybe 1 of 100 of these investigations do little more than get filed away, that one could cost the company hundreds of thousands or millions of dollars. This is not an exaggeration. There are many cases throughout this book that could be used for this training.

Once the awareness is engrained, technical training must be provided. (Training is covered in more detail in Chapter 6.) Officers should be shown to document everything as they see it upon arrival. If possible—if it is not an emergency—the first officer should look carefully at the overall scene. In a guest room, he should note the condition of the door, the items in the bathroom, signs of struggle or accident, other persons present, etc. A camera is the best way to document and can be a good way to jog an officer's memory later, but notes should still be taken. The camera will not capture sounds, verbal statements, smells, and even lighting conditions. Taking notes is not that simple. It is difficult for anyone to know what he or she should write. As mentioned previously, just write down everything. It helps to have another officer who can take statements and discuss the situation with the guest while the first officer concentrates on documentation.

Response

Remember that our first objective when responding to any incident is guest safety. If they are injured, we get them appropriate medical attention. Our second objective is to provide empathy. After the well-being of our guest is stabilized, then we can begin gathering information. So an abbreviated response should sound like this:

1. Are you OK?
2. My gosh, that must have hurt (or been scary) or whatever.
3. What happened?

Medical Response is covered in 7. The timing of calling EMS is dependent on your jurisdiction. In the US ambulances are either private, under contract with the city or county, or part of the Fire Department. There are some rural areas that are different. The reason I mention this is because we have a duty to get medical attention to the guest as soon as possible. Strokes, heart failure, and certain head injuries depend on every minute to avoid permanent damage and death. It may behoove you to call 911 as soon as you know you have a serious injury or illness.

Once the medical situation is stabilized, we offer some empathy. This is difficult to script, and the style depends on the employee. As a representative of the property, we never want our employee to take responsibility for an accident, offer their opinion, or provide too much information. Avoid statements like:

Oh, this happens all the time. Don’t worry, the escalator company usually pays for these accidents. Again? We need to get that carpet replaced. I saw the kid spill his drink in front of you.

Statements that are acceptable:

I am so sorry this happened to you. Is there anything I can do for you? Can you tell me what happened? Oh, that must have been frightening.

I tell my employees that this is another leg of guest service. Treat the guest as if they were in your home and they tripped and fell. How would you interact?

Take note of the spontaneous statements made by the guest. “My darned knee went out again.” “My husband walks so slow I ran right into him.” “I am always scared of escalators.”

Starting the Investigation

If you have someone to start taking photos while you tend to a guest, that is preferable. If not, avoid taking photos of a guest who is on the floor, in a precarious position, or on a gurney—guest service first. The other associate can start collecting witness information. If not, the first officer will have to take note of who is there and follow up after finished with the guest.

Photos

The more photos, the better. We want to get a shot of the guest if possible for video review later—on slip and falls, the shoes, assist devices like canes, luggage they were carrying, etc. The accident scene with or without the guest is next. Make sure the spill is documented before it is cleaned, or the hazard before it is repaired. An overview would be next, showing the scene in relation to landmarks. Anything else would be helpful.

Witnesses

There are two realities that they do not teach in report writing class. One is that bystanders are eager to stick around and take credit for the assistance they provided, but rarely want to "get involved." Two is that first responders, including security, are shy about interviewing witnesses I have no explanation for this. As a compromise, instruct your responders to talk to witnesses at a minimum and get a name and phone number so we can call them if necessary. That is usually acceptable to the shy security officer and the passive witness.

Interview

Once the scene is "preserved," at least in memory and in photos, the next step is to reconstruct what happened. This is accomplished by first obtaining a verbal account from the "victim" and then from any witnesses. Allow them to verbalize the story, separately if possible, and before they write it down. As they recount their experiences, let them speak uninterrupted as you take notes. After the verbal statement is given, ask questions to clarify or understand. Then repeat it back from your notes. "So, you used your key, walked in the room, and saw the suitcase lying upside down on the floor right about here." If they then change the story, note the change. Then have them write the statement. Once you have the statement, compare their verbal and written statements for clarification. "You told me that you used your key to open the door, but your wife said you lost your key and used hers." (We are not interrogating, just asking for clarification.) Once you have their statements down, compare the story with the evidence. "You said the suitcase was upside down on the floor, but it is now on the bed." This goes on until we have his story, her story, the maid's story, and our story (what we saw). These will be put together in the report. This process is necessary to get a more accurate depiction of facts. Invariably, once someone has time to think about it and speak to others, their recollection changes. A $50 watch missing from the room may turn into a $1,000 watch by the time the statement is written. We do not accuse the guest of lying or changing their story, we just want to clarify. Take note of the relevant parts of this discussion and include in the report.

Evidence

There may be items associated with an incident that are relevant for the case. I am not talking about counterfeit money, drugs, or bullet fragments. That is for the police. I am talking about a cocktail glass that is cracked and caused an injury or a piece of flooring that came loose. Get with your risk person and find out if they want to save these items or if photos will do. The industry, especially the large properties with the resources and volume of cases to do so, keeps evidence.

If you do keep evidence, this is where you get to use those police skills from TV. We want to keep hands off it and preserve it as it was found. Photograph it where it was found, then store it in an appropriate container that keeps it from being damaged. You may keep this item for years. Zipper plastic bags, pill containers, paper bags, etc. Seal it so that it cannot be opened without damaging the seal. Transport and store it using as few persons as possible. Document the handlers. This is known as "Chain of Evidence" and could be important if the item is used in a trial. An opposing party may claim the item is similar but not the original one. Again, Security will look bad.

Check with your legal folks to see how far you want to go with evidence. They may recommend anything that is moveable, or they may say to keep only certain items. Once the item is preserved and stored, it may be kept until Legal releases it. This is usually a year after statute of limitations (in your state) runs out. If it is a minor, be prepared to keep it until the minor is an adult.

I honestly had someone slip on a banana peel once. We kept the evidence and asked the attorney about perishable items. He asked that we keep it. After the litigation, he said the judge and the plaintiff were impressed and stymied that we kept a banana peel so long. They had no doubt it was a genuine cause of the accident.

Drugs and Contraband

Note that our evidence is collected for our use, not a prospective plaintiff or the police. If the police need it, they will take it. Therefore, I recommend not storing contraband or drugs. Weapons should be turned over to police or disposed in accordance with your found property procedures. Drugs, stolen merchandise, and other criminal items need to be placed on someone else's back.

Once the statements, photographs, and evidence are gathered, the preliminary investigation is complete.

REPORT WRITING

Let's get a couple things straight before we dive in. Incident reports are necessary for the company to have documentation of what happened. The information contained therein may be used in litigation, claims, policymaking, and discipline. Our reports are NOT for crime prevention, apprehension, crime statistics, guest insurance claims, or the "guest's records." Guests will assume that if you take a report, it is the same as a police report. It must be explained to the guest that our report is for our records to "notify management of what happened."

Therefore, a guest who wants to "file a report" should be referred to the police. As far as an internal report, they have already notified you and that is a report—as far as they are concerned. Guests will also ask for copies of a report involving them. This is a bad idea and should be avoided. Our report, hopefully, is not going to be as empathetic, may incriminate the guest, and would provide ammunition for them to make a claim against us. The only copies we give to patrons would be the statement they signed. Otherwise, they are on their own.

Reports may be seen by supervisors, department heads, police, lawyers, prosecutors, juries, and judges. This needs to be stressed to the report writer so that like the preliminary investigation, the report is thorough, detailed, and accurate. Report writing is arguably one of the most important functions of the Security Department, so even though you have given and received training on it, I am going to go over the important stuff.

Officers should be hired and trained with the objective that they will write reports based on incidents that they see. Having supervisors or specialists write the reports works for some but is awkward. It is difficult to write a report in the first person if one is not at the scene. Supervisors are trained and paid to take more responsibilities than this frontline duty, so this process is inefficient. Hiring officers who can already write is a big help.

Format

Your company may require a certain format for incident reports. Otherwise, the industry has a best practice that loosely follows police reporting. First, we list statistical information. This is often from a menu that uses these fields for searches and reports. Whatever is not included in the "boxes" should be noted before the narrative. Note that we do not use suspect and victim because this is not a crime report. This data includes persons mentioned (name, address, description, etc.); lists of missing items, damage, etc.; description of each photo (location and time taken, subject of photo); video included with report should be catalogued, as to camera number, time frame, location, and brief summary of contents. Evidence is also listed (with location found, description, relevance, and place stored.) Finally, a list of all attachments to report, the attachments, including all of this information in a narrative format, makes it cluttered and difficult to read.

Almost every incident has photos. We already discussed how and where to take them; now they must be documented in the report. The photos should be listed before the narrative with a number that corresponds to the photo or file name. A brief description, name of photographer, location, date, and time taken should be included in this list.

There are a couple of theories on video review. Some companies have the responding officer do it. This helps he/she understand the incident and jog their memory when writing the report. It also saves others' time in doing review. It is important that officers not reveal video results to a guest. Other companies have the investigator review video. Generally, he/she is more experienced, understands some of the nuances to watch for, and may find the video more resourceful. The person who will review video is dependent on your staffing. This is a time-consuming process, so it may come down to whomever can afford the hours involved. I recommend a compromise of these two methods, have the officer find and preserve any relevant video, locate times and locations that are pertinent, and then turn it over to the investigator for a more critical review. Whatever the officer sees on video should be included in the narrative.

Narrative

Rather than go through an entire writing course, what follows are what I consider necessary for reporting incidents. Like every other process I have explained in this book, the same applies here: Establish your objective first. For reports, that means, who is your audience, and what facts are you trying to convey? Your reports may be for management, they may be for other departments to take corrective action, and mostly, your reports will be for investigators to fill in blanks and for Risk to speak to the guest involved.

Because of our audience, we do not include opinions and we need to be careful not to include information that could hurt us later.

In my experience, it is better to get the account of the first responder for the report. Our frontline workers sometimes struggle with this. After all, they did not become a security officer for their writing skills. In fact, many bow out when they find out about some of the administrative work involved. So there is a bit of gray area here as to what is acceptable. A report can go all the way to a courtroom, but generally goes to management and maybe your legal team.

This part is much easier than everyone makes it out to be. The narrative simply tells a story, in chronological order of what the writer did from start to finish. It should be done in the first person (use "I" instead of "Officer Jones" or "This officer"). These are outdated forms of writing and are difficult for a layperson (like on a jury) to read and understand.

The narrative starts at the beginning (from the writer's point of view): On this date at this time, I was dispatched to … Or: On this date at this time, I saw… . As the narrative continues, it is easiest to tell the story from the eyes of the officer as it happened. "When I arrived, I saw this, I did this, and this person was doing this and then I did this. Mr. Guest said that this happened, then I spoke to Miss Customer and she told me this happened." On and on it goes until the officer leaves the scene. Then she continues writing whatever follow-up she did—gathering statements, room information, lock interrogation, etc.

Corrections

Those writers with poor grammar and spelling are not off the hook. We need their first-hand account, which will likely be taken in a deposition anyway, so whatever their writing skill and style, stick with it. There are still some areas where we cannot compromise.

I have tried using designated report writers and this is fine but not preferable. The first observations of the first responder are really vital, but sometimes get muddled by a second person. I had an officer once who was dyslexic (confuses the order of letters in words). He really struggled and always had a dictionary with him, but it worked. I also had an officer who had trouble forming sentences and paragraphs. He used his own templates for the basic reports to remind him the order of information. He rarely left anything out. If either of these guys went to a deposition or a witness stand, I would not be concerned. They could both verbally represent themselves well and I would advise them to be honest about their writing skills. No harm there.

Officers should correct their own reports by proofreading them. Spell check is a good tool, but the wording and grammar should be their own. Using big words or words they do not understand will cause problems later if they are deposed. Their own wording should be used as long as it is accurate. I am not saying to use slang, profanity, or gibberish, but it is not necessary and does not sound like normal conversation to use words like "approximately" and "expedited" when "about" and "hurried" will do. If your writer uses the wrong verb tense or spells "received" incorrectly, let it go. The writing, combined with a deposition will speak for itself—as long as the facts come across. Do not worry much about context. If a report is unreadable, that is different. Some practice may be in order before writing a real report. Dictation is not out of the question if you have the opportunity.

> Officers who are self-conscious about their writing ability will sweat, stall, and struggle through this process. Ask them to stop writing and tell you what they did on the call. They will likely tell you a story like the one I related before. Perfect. Now write exactly what you just told me. They are likely stuck on the big words and what they think we want to see. When it dawns on them that a story in their own words is what we want, it makes it as easy as writing in a journal or diary. When they get to that part, we just fine-tune the edges with such things as photos, video review, etc.

First Person—The old style of third person writing has almost entirely disappeared but you may still get a retired police officer or someone who is used to writing this way. Third person is difficult to follow and confuses everyone. Stick to first person: I arrived on scene at 12:00 and… I found the banana peel near the guest's left leg… I placed my hand on the man's shoulder to guide him to the door…

Attachments

Numerous documents having relevance to the report should be attached directly to it. Do not presume that other departments will hold the info for you or that it will be attached later. Some attachments that are common in hotel reports are the statements from guests and victims, the room folio, lock interrogation report, reports from housekeepers and engineers, and any other paper document that is necessary to support the report.

The written report with supporting video, photos, statements, and other evidence concludes the preliminary investigation. I hope that you have an investigator who can follow up on it if necessary.

Next Steps

Depending on the preference of your management, reports may be disseminated to the big boss, legal, risk, investigations, and the affected department head. Beyond that, you should keep them confidential. Reports, in my mind, are the product of Security. Your integrity and skills are judged with each one. Make sure your reports are complete and accurate.

Retention

Unfortunately, the huge majority of your reports will be filed away and never seen again. That does not mean they are not important. Reports are like insurance. Make sure you have back-ups and safe place to store them for years. The retention of all your documents will depend on your Risk manager or possibly the CFO who is responsible for all records. They will generally advise a 3-year retention. This allows for the statute of limitations with some cushion. Reports involving minors may have to be kept until the minor reaches 18 or 21.

Nothing is more detrimental or embarrassing than looking for a report two years after the incident and not finding it. Keep your back-ups as secure as your originals.

Keep one copy, perhaps electronically, offsite (in a cloud server) in case of catastrophe on property.

Report Writing Software

I have even the evolution of reports from writing on lined paper in block letters, to typewriters, to word processors, to homemade databases, to third party software solutions. The latter is where you need to be, if not already. It does not matter much for the report itself, but searches and data are impossible to derive without a database. The next steps, already being used in some places, are tablets which are used to obtain the photos, statements, record video, and dictate a narrative. These may evolve into video records of everything.

In choosing your software, consider scale, upgrades, simplicity, and data handling. For example, I used one that had "canned" reports that were not useful for me. I wanted to create my own, but it was not possible with their platform. I have used others that were so complicated; the front line could not use them without much practice. You need something that can grow with you and is supported by the company. If you had something that also provided other functions like Lost and Found, Dispatch, Daily logs, Pass down and maintenance, it would be an advantage.

INVESTIGATIONS

Investigations in the Hospitality industry are usually considered somewhat reactionary, where the investigator follows up on certain reports to "solve" them. This is only partially true. If you limit your investigators to follow-ups, you are severely limiting their capabilities. These are some of your most well-trained, highly skilled employees and their talents can be put to work in other ways that benefit the property. In this chapter, we will not only discuss how to recover assets, but also how investigators compile data, analyze it, and enforce vulnerabilities.

Consider first your volume. If you have a quiet 200 room hotel with little or no meetings, one restaurant and one gift shop, you likely do not need a dedicated investigator. One thousand rooms with a mall, theater, and casino better have one. After volume, look at potential. If your risk manager could settle more claims—in the hotel's favor—with a proper investigation, then the additional staff might pay for itself. Finally, you may be negligent if you cannot keep up with investigations. For example, you may have a rash of robberies in your parking garage. The police may or may not thoroughly investigate, but your own person may find the common denominators to either lead to an arrest or to recommend measures to be taken to prevent the attacks. If a guest decides to hold the hotel accountable for their loss, it might be negligent for you to have had the chance to mitigate these crimes but did not have enough staff.

Unlike police detectives, the objective of a hotel investigator is not to prove (or solve) a crime, but to protect (or recover) assets. Call this your "Loss Recovery" unit to keep the focus on the objective. Recovery, in security, is most often accomplished through report follow-up. In most cases, security officers generate reports. (In some cases, investigators will initiate a report from information they received directly. This is discussed later.)

Report Follow-Up

The previous section covered the preliminary investigation which documents the event as it happened or just after it occurred. It compiles all the information an investigator needs to continue the process. I am hearing some security directors saying they barely have the staff to minimally serve the guests as it is. How will I afford an investigator? I understand and offer some compromise.

It is the investigator's role to review reports for thoroughness, extract statistics, and monitor incident trends. He should not be looking for grammar, punctuation, and sentence structure (that should be done by a supervisor) but needs to flag reports that are lacking in information he might need for an investigation. If there is video missing or a witness statement that was not included, these need to be attended to immediately even if the investigation has not started.

The investigator extracts statistics that will be important for crime analysis and risk assessments (later in this chapter) on all reports. As for follow-up, this is done on those reports that meet certain thresholds set up in advance with the director of security. Thresholds (or triggers) are established based on the staffing levels—how many investigators to handle how many incidents—and what reports are worth solving. If there were ten missing property reports per week and only one investigator, you might raise the loss amount up to reduce the number of reports to investigate. On the other hand, if your claims representative were going to automatically pay claims less than $50, it would not be worth investigating values less than that. This is not to say that these losses are ignored. You will still track them to see where they fall in your Risk Assessment and to see if there are any commonalities, such as the same valet attendant or certain room numbers, and so forth.

Thresholds may get more complicated depending on whether there is enough evidence to conduct an investigation, the workload of the investigator, if the suspect is an employee, if there is liability on the hotel, etc. Whatever the thresholds are, they should be documented so the investigator may apply each report he sees to the criteria and make a quick decision to close the case or leave it open. There also should be a regular meeting, perhaps weekly, between the investigator and the Director to discuss the cases and determine whether they should be investigated based on workload, other investigations that have occurred, or input from the General Manager or Risk Manager. Triggers are discussed in further detail later in this chapter.

Some incidents will be investigated every time, such as sexual harassment, employee theft, discriminatory offense, or law enforcement (criminal) involvement. Set those criteria in advance as well or handle them on a case-by-case basis so they are not overlooked. Types of investigations vary depending on the incident, so we will go through each type you are likely to encounter at your property.

You will likely be investigating five types of incidents:

Internal—Any incident involving an employee as the suspect (offender) or as the victim (complainant). This would include most property losses, damage, employee theft, and guest complaints.
Criminal—Any incident where the police or a law enforcement agency will bring charges against an employee or guest.
Accident—Guest accidents and injuries. This includes food poisoning claims, bed bugs, etc.
Workers' Comp—Employees injured in the line of duty and work-related illnesses. Accidents, food poisoning, carpal tunnel, second-hand smoke, etc.
Personnel—Incidents involving employee misconduct, such as sexual harassment, intoxicated on duty, and employee complaints.

The investigator will have to determine the type of incident, who will do the investigation, and the type of investigation. These types are based on the expected outcome:

Personnel—Might result in disciplinary action or term
Criminal—Could result in criminal charges
Workers' Comp—May result in claim denial
Guest Claim—Determine fault of company

Personnel Investigations

Personnel investigations generally involve some sort of misconduct. It may be theft, sexual harassment, or assault. For our purposes, we should not get involved in minor infractions such as poor performance, absenteeism, or guest service issues. Leave those to the department head. Before starting a personnel investigation, keep your eye on the ball. Your investigators' objective, like yours, is to protect the company's assets. The way we do that in a sexual harassment investigation is to be sure that the company bears no blame for the incident. "Company" means supervisors and managers who act on behalf of the company. If your company is perceived as being ignorant of these types of incidents and allegations, they could be liable for the incident or past and future incidents. Therefore, besides making sure your "victim" is safe and free of harassment, you need to be sure the company did not do anything to cause it and is taking steps to stop it.

The first consideration of a personnel investigation is who will do it. Many HR departments prefer to conduct their own investigations. This is fine, but make sure their investigators are trained in interviewing skills. Smaller organizations hire an outside investigator to conduct these. I prefer Security to do all investigations, not only because of the training they have, but because it is a "third party," which allows HR to make an unbiased decision. A second consideration is consistency and fairness among all employees. HR and some department heads will think they have an easy case (two or more witnesses saw misconduct) and will make a termination decision without an investigation. This is often not a problem, but this employee may have a case against the company if he can show you a full investigation required by Security with other employees and not him. On the other hand, the employee who is terminated after a thorough investigation with interviews and an interrogation may claim discrimination because the other employee was not subjected to the same treatment. Establish a system with your HR Department that puts all employees through the same type of investigation, so your actions are perceived as fair.

In 2008, a restaurant worker, who had been sexually harassed by her boss, sued the restaurant for hostile working environment. The restaurant had completed the investigation within two days of the first report and fired the harassing boss. The court ruled in favor of the restaurant because they had taken thorough and quick action against the offending supervisor.

> A consistently enforced policy and thorough investigations can help a company defend itself from these types of suits. Sloppy or slow investigations can lead the victims to believe that management does not buy into their own policies or that management is trying to cover for its unacceptable behavior.

Written statements are usually the first step in any investigation. Statements should be obtained from all parties in the incident. This is a common way for the investigator to receive the investigation. A manager hands him the statements and he does the rest. (Don't complain about this—the less done on your behalf, the better.) The initial statements will likely be from the "victim" or the one making the complaint. There also may be a "suspect" or offender statement. If these statements have not been written yet, do not obtain them. A good interviewer will get better information verbally and nail it down with the written statement afterward.

It is common, in our culturally diverse environment, to get statements written in a foreign language. Do not trust other employees to translate this for you. Friends and co-workers will not provide an accurate translation and will insert their own opinion of what they think the victim should have written. Have a prearranged Security or Human Resources employee to do this for you.

Verbal translations should be handled in the same way. Do not use the employee's supervisor or co-worker to translate for you. You will need a qualified translator—at least an unbiased one.

The next step in an investigation is to gather evidence. Evidence includes any item or piece of information that will prove or disprove any part of the incident. This may be video, email, personnel files, policy excerpts, and prior cases. Each of these items needs to be reviewed, documented, and filed with the report.

Video may or may not show the incident as described, but it also may be used to prove that the incident did not happen as alleged. It is useful as well for identifying witnesses that can be interviewed and to prove witnesses actually saw anything at all.

Email and other computer data are invaluable in many types of cases. This information should be saved in its data form and on paper to include with the report. Do not rely on the department or Information Technology (IT) to archive this for you. This data can be easily misplaced, and your case lost.

Personnel files may or may not show previous related incidents, such as a pattern of behavior or a tendency to make false reports. They also may contain policy memos that were signed by the employee prohibiting that behavior.

Policy excerpts are necessary to justify your case. If you are investigating sexual harassment, include that policy to show what your case is proving.

At this point in your investigation, having reviewed the available evidence and statements, it is time for a management conference. This is usually between HR, the department involved, and the investigator. This is a chance for everyone to understand how much proof will be needed (this is discussed later) and what type of proof—a confession, two corroborating accounts, certain wording in an email—and what the expected outcome will be—termination, suspension, discipline, remedial training, etc. The investigator can also pick up some negotiating tools to use in his interrogation. "If you admit to this and undergo some counseling, I might be able to get you off with just a suspension."

Interview

An interview is part of the fact-finding process. There are nuances in an interview that require a trained investigator. Knowing what questions to ask, when to ask them, and observing the person's body language is important so do not let another manager or HR person conduct the interview. Note that an interview is not an interrogation. This is a time for the investigator to set up a rapport with his subject, without making accusations or coming to any conclusions. Notes are taken, but it should be audio and video recorded with the camera facing the subject. There are interviewing and interrogation skills that require specialized training and every person who conducts these processes should have that training. We will touch on some of it, but this chapter does not replace that training and a lot of practice.

Victim

We usually start with the victim first. This is not vital, but it just makes more sense to get the original complaint directly from the complainant, so you understand exactly what you are investigating. The interview is nonconfrontational and a chance to get the victim's side of the story. Just as was done in the preliminary investigation, questions are asked, and answers repeated to clarify. Note: I have seen many company investigators perform this initial interview like an interrogation, accusing the employee of causing the problem, and deriding them for wasting his time. You do not want this type of rapport with employees. Let them know you are trustworthy and sympathetic. This will earn their respect and trust, and word will travel quickly that you are one they can go to for help or to report someone else's misconduct.

During the interview, the investigator is doing several things. First, he analyzes the written statement and compares it to the statements made verbally. Second, he examines body language. This is not quite the same as what you see on TV. The concept is to determine someone's truth-telling style by noting their body language and mannerisms when they are telling the truth, then comparing that style to answers given later during questioning. Third, he is deciding what questions to ask to extract more information on certain points that arise.

During the interview, the investigator also will introduce questions that arose from reviewing evidence. You said it happened here, but the video shows it happened elsewhere;

tell me more about that. Your statement says that there was nobody else around, but an employee told me she was there the entire time and saw nothing; tell me more about that. Once again, there is some great comprehensive training available on this topic and it is highly recommended.

In conclusion, always tell everyone involved in an interview two things: (1) false accusations or false statements and refusal to cooperate with an internal investigation can result in termination, and (2) the interview and investigation are confidential and revealing the content thereof is a violation of policy.

Witnesses

Witness interviews are handled the same as the victim interview. Either their story will corroborate the victim, or it will not, so you will need to delve into those conflicts. They may reveal important details that the victim left out. A witness can turn an investigation upside down, revealing a conspiracy to get the suspect in trouble, so keep an open mind and cull the facts. Witnesses should be admonished just as the victim was on disclosure and cooperation.

Non-witnesses

You find these people without the help of the victim. A non-witness is someone who was at the scene but says nothing happened. These people can also reveal a conspiracy and have no motive to lie.

Character Witness

A character witness is someone who can vouch for the validity of the incident or the history of any one of the subjects in the investigation. They may be able to tell you if the two employees had a previous relationship if you are investigating domestic violence or sexual harassment. They may be able to tell you about their financial status if you are investigating an embezzlement case. Although they may not have witnessed any misconduct or an actual incident, their historical information may be relevant.

Suspect Employee

The last person to be interviewed (at least in the first round) is the suspect or the accused employee. If the employee has not yet written a statement, it is better to hold off until the end of the interview. The reason for your interview is to get their side of the story. So, this interview should start out and remain friendly. The interviewer needs to build some trust and some integrity by reminding the employee that he is just doing his job, just wants the truth, wants the employee's side of the story, and may be the only person who can help him.

The employee should tell the story uninterrupted. During this time, notes are taken with careful attention to truth-telling style; gaps in mental timeline, at which points in the story the mannerisms change, parts of the story that do not match; and parts of the story that are left out from the witnesses' or victim's story.

The truth-telling style was explained briefly before, and I cannot stress enough how important it is to have extensive training in these techniques. For the sake of the Security Director who needs to know what his investigator is doing in those interviews, I am summarizing it here. The interviewer pays close attention to the subject's telling of the story. It is better to have him start at the beginning of the workday and tell what he did from the moment he arrived on property that day. This gives a chance to identify the subject's truth-telling style. This style is displayed as he tells the truthful part of his day (where he parked, what he had for lunch, etc.). The interviewer notes his body movements, posture, facial expressions, etc.

As the dialog gets to the point of the alleged incident, we watch for changes in the body language, voice inflection, and so forth. These may indicate lies. We also listen for gaps in the timeline. There may be much detail as he recounts each hour of his workday, then breezes through the 15 minutes when he was in the storeroom drinking beer. It is more difficult to recall a lie, so people tend to leave out detail, so they are not caught up in the lie. Once again, this may be an indicator, but it will be worth more investigation.

When he finishes his story, the interviewer goes back to the areas of concern. Whether it was a gap in the timeline, a different body language, or a difference between his story and the victim's, probe that area and repeat back what he said and say, "Tell me more about that." Do not tell him which part interested you; just ask him to talk more. This is done several times, continually narrowing him down or leading him through a complicated lie that he cannot get out of and that you know is not true.

Once this process is concluded, there should be some idea in the investigator's mind of whether the subject was being truthful. That is when you have him write his statement. This often puts him at ease that he is out of trouble because you could not get anything out of him. Do not prompt the statement; just say you need him to write everything that happened between 3 and 4 p.m. or everything he did in the storeroom up until he went to his locker.

Post-interview Conference

At this point, there is a pause in the investigation as the investigator reviews his findings. He either knows the employee is "guilty" or has learned new information that needs to be checked. If the latter is the case, the investigator goes back to evidence or more interviews until he has resolved all doubts or questions. If the investigator has already reached his conclusion, he will need to consult with his director, the HR director, and possibly the department head. This conference is used to review all the findings and determine the next steps. (See "Burden of Proof" later in this chapter.) Someone will decide if there is enough evidence to stop the investigation and issue discipline or termination, or whether it will go unresolved with no discipline. It may be determined that everyone believes he did the act of which he is accused, but they want a confession. This is done through an interrogation.

Interrogation

The interrogation is somewhat different from an interview, and only necessary if there is not enough evidence. To begin an interrogation, the interviewer knows the subject is guilty, but does not have enough evidence. A confession is the goal of an interrogation. The interviewer does almost all of the talking and spends some time telling the subject how much evidence he has against him—statements, video, witnesses—he just wants to know why the person did it. Or he just wants to recover the money, or some other secondary concern. This takes some time to engrain in the subject's mind that guilt is no longer a doubt while he will deny it. Good interrogators use several styles to achieve the confession. They may use guilt, such as "What is your family going to think?" or they may be empathetic, "I know you just needed the money to feed your kids. I might have done the same thing in your position." Or, they may try promising them leniency, "If you just tell me how you did it, I can talk to my boss and maybe we won't press charges." There are many techniques, and you may have to use them all for hours until the subject finally sees no way out.

A California employee of a large manufacturing company was called into the office and accused of theft of company parts. He was forced to drive the investigators to his home and submit to a search for the missing parts. The man sued for false imprisonment and invasion of privacy and was awarded $214,000.

Investigators have no authority to search a person and his property without consent. Care should be taken not to hold someone against his will and certainly not to physically force him to do anything. During an investigative interview, the only authority an investigator has is over the employee's employment.

Forget the cop shows and remember the following: We are not enforcing laws or prosecuting crimes. We are simply determining policy violations. Therefore, we do not read anyone their rights, we do not hold someone against their will, and we do not handcuff them. (If your investigation is leading to a criminal investigation, back-off and let the police handle it.)

Resignation versus Termination

Many companies will accept a resignation in lieu of an employee being terminated. HR Directors prefer this for many reasons. One is that their unemployment insurance may not have to pay on a resignation. This is hardly true anymore because employees can claim they resigned under duress. Two is that they believe they will save time and money if the employee decides to challenge his termination with a labor agency. This is also no longer applicable for the same reason. Three is that they are not comfortable with the evidence provided. It is generally not up to Security to make this decision or to accept a resignation. Whatever your HR Department decides, make sure your investigation is complete and accurate and includes all of the evidence even if you think you will not need it.

In 2010, a warehouse worker at a Connecticut beer distributor was being questioned about stolen beer. Investigators showed him video of the theft and offered to let him resign. The man calmly refused, asked to use the restroom, and came out with a handgun he had hidden in his lunch box. Nine people died.

Investigators should remain calm and friendly, but never let their guard down despite an employee's demeanor. This situation was avoidable and may have been prevented with some of the policies discussed in Chapter 7.

Remember that confessions are not necessary to prove or resolve your case. Later we will talk about the burden of proof required in a hotel investigation and restitution, which is our main objective.

Cooperation

When the police interview a suspect, they must advise him or her of certain constitutional rights. We sometimes must remind ourselves that we are not the police and do not have to do that. Our interviews are with employees and their participation is a condition of their employment. You should have a policy to this effect in your company policy manual, and you should remind employees of this when talking to them. Of course, they are free to leave at any time, but doing so will be cause for termination. It is advisable to tell them that before beginning an interview. This is a good time to remind them that lying or refusing to cooperate also may be cause for termination.

Having provided these admonishments, make sure the interview scene is nonthreatening. Do not back your subject into a corner where he feels he cannot leave. This could come back to you as false imprisonment or unlawful detention. There is nothing wrong with offering water, tissues, and restroom breaks. The old tales of the wobbly chair, bright lights, and threats of violence are reserved for the movies.

Unions

If your company has any employees in bargaining units, chances are they have wording in their contract allowing a shop steward to be present during interviews. A rule derived from The Weingarten Act provides any employee who is questioned by any member of management, where the questioning might lead to disciplinary action or termination, to have an employee witness present. The details of this agreement depend on the specific contracts in place at your property, so you should consult your HR Department. Failure to provide the shop steward during your interview may invalidate the information received and cause a union grievance to be filed, or worse—an unfair labor complaint. Once you establish this procedure with HR, make sure you follow it the same way each time you interview a union employee. In most contracts, the steward is not allowed to give advice or even talk, so it is not a big deal. In fact, you may be able to select the steward.

Translators

We mentioned earlier, regarding statements, that the translator you use should be one of your choosing who has training. What I have seen in most instances is the translator plays lawyer and speaks on behalf of one party instead of just translating. You can imagine how this can botch an interview where you are trying to reveal lies in the wording or certain statements that make the employee nervous. Even with a good, trained translator, it will be very difficult to do a good interview or interrogation. In a perfect world, you would have a bilingual trained investigator.

Burden of Proof

In a personnel investigation, we are not proving a crime, only a policy violation. We do not have the same burden (beyond a reasonable doubt) that has to be proved in a criminal setting. This is why we go for violations of policy rather than breaking of laws. For example, if you are investigating a theft (loss) from a storeroom, you only need to know that your suspect was in an unauthorized area, did not follow requisition procedures, etc. If you had to prove the actual theft, you would need a video camera or a witness who saw the suspect put the item in his pants. Suppose a guest complained that an employee shoved him. This may be a criminal battery. To prove that the battery occurred, you would need a witness, video, or something more definite. Unsuccessfully prosecuting an employee for battery does nothing for the hotel (or anyone else), but we can easily prove that he violated a guest service policy, was out of his work area without permission, had inappropriate contact with a guest, or any number of policy violations.

Because policy violations are not misdemeanors, they do not have to occur in our presence to terminate the employee. Since our property is not a court of law, we do not have to prove beyond a reasonable doubt that he did it. Most internal investigations will result in a policy violation or the discovery of a flawed policy.

> In O.J. Simpson's murder trial, the prosecution was not successful in proving beyond a reasonable doubt that he committed the crimes, so he was acquitted. In the subsequent civil trial, he was found to be responsible for the murders. Civil trials have a different burden of proof called "preponderance of evidence." This is substantially less proof required and is therefore easier to prove. For the sake of this illustration, suppose Simpson was our employee and we wanted to terminate him because his involvement in the alleged murders was damaging our reputation. We would have many policy violations, not even related to the murder, that we would use to successfully terminate him.

Criminal Investigation

During an interview of what you suspected was a personnel investigation, the case may turn into a criminal investigation. For example, what you thought was a sexual harassment allegation might turn out to be an alleged battery or even sexual assault. Naturally, you would notify law enforcement as soon as you find out. The danger in continuing a suspect interview may cross a line of acting as an agent of the police. All kinds of legal ramifications come into question, including should you now "Mirandize" the suspect; is the information you receive now protected by the Fourth Amendment; and is the suspect still free to leave. Better safe than sorry—inform the suspect you are calling the police and turn over everything you have to them. If you have enough to arrest the suspect to keep him from leaving, do so. The investigation now becomes a police matter, and your HR Department can make a decision based on their outcome.

Keep in mind that your investigation may have to continue—without the suspect—to cover any civil liability. Even though law enforcement action may seem to take this to a certain level and out of your hands, the company may still be liable for a hostile work environment or something else depending on the original allegation. So, you will want to stay in touch with the detective or prosecution as it relates to company liability.

In order to stay in contact with the investigating agency, you should develop a supporting role. This means supplying video, handing over statements you already have, and seeking witnesses and evidence. Be sure to consult your counsel on what level you will cooperate with police. There may be proprietary information that must remain private and is subject to subpoena. Finally, make sure to keep copies of everything you give the outside investigators. If their case falls through or even if it does not, you may have to run a continuing, or parallel, investigation of your own.

Private versus Public

Many people in both private and public sectors have trouble distinguishing the difference between private and police investigations. The objective of a police investigation is to prove that the suspect committed a crime. Even if the investigation objective is to find a suspect, it is done knowing that a crime occurred. While there may be crimes occurring at your property that require investigations, keep reminding yourself that you are not the hotel police department. Your objective is to protect the assets of the company. This is not to say that you cannot resolve guest issues and retain your customer. You may owe them that much, depending on what the problem is. After a loss has occurred, the only way to protect assets is to recover the loss and to prevent future losses from occurring. This is a novel way of thinking for some of us who have been engrained to solve crimes and catch bad guys.

If a guest suffers a loss, it is the investigator's job to either prove that it was not the fault of the hotel or recover the loss. For example, if a guest is missing his or her laptop from the room, and we can prove that no employee took it, and there was no responsibility for the loss, such as a faulty lock or no security, then the hotel has no exposure.

Restitution

We have talked throughout this and other chapters about recovering losses. This is commonly done through restitution. Restitution can be a valuable interrogation tool and a metric for showing security's contribution to the bottom line. It is generally a negotiated amount up to or equal to the amount of the loss. It can also include administrative, labor, investigative, and other costs associated with the loss.

During an interview, a common tactic is to use restitution as a bargaining tool. An employee who thinks he is facing criminal prosecution may be very willing to pay back what was stolen or damaged. The investigator can negotiate on the amount and even payment terms in return for other information provided. Remember, this is a private agreement and has nothing to do with the crime or the police. That also means it will be harder to collect. You should try to get the majority of the amount out of the employee's final check because it is not likely you will see him again.

Court-ordered restitution is also a very viable source of recovery for the Security Department. An employee who is being charged with embezzlement or a "guest" who is being charged with theft can be responsible for restitution. This will depend on the initiative of the police officer making the arrest report, the detective who prepares it for prosecution, and the prosecutor. If all of them work with information you provide, the judge is likely to order restitution if the suspect is found guilty. Your department should have restitution letters that are filled in when an arrest is made. Include the loss amount and any associated costs with the arrest. Don't forget the labor costs of the arrest, the administrative costs of processing the report, and any other department costs. It is best to have these costs itemized in a list in advance, so the arresting officer can put these into a letter to go with the police.

WORKERS' COMPENSATION INVESTIGATION

Security is not always the department dubbed to do employee accident investigations. I believe it is only natural for Security to use its trained investigators for this, especially because it may reveal employee misconduct or flawed safety policies. The Workers' Compensation Department, HR, or the insurance company usually initiates these investigations. If the explanation of the accident appears doubtful, if there are some suspected safety or policy violations, or if the employee is suspected of insurance fraud by making a false claim, an investigation is likely to be requested.

The process is very similar to the one for personnel investigations discussed earlier in this chapter. There may be different forms and report formats and the burden of proof may also vary, but the fundamentals are the same. As we proved a particular policy violation in the personnel investigation, for accidents we focus on four main conclusions:

1. Is it work-related?
2. Are there any safety violations or recommendations for future safety policies?
3. Was it caused by the employee, the company, or a third party?
4. Was there negligence on the part of the employee?

Each of these can cause a claim to be denied, partially paid, or deferred to another party. The insurance company will generally direct you to its main concerns. Regardless of what the insurance company decides, you may be directed by HR to find policy or safety violations that they will address.

GUEST CLAIMS

The fourth type of investigation involves guest claims. These claims (whether there is an actual claim or not) include guest accidents, loss or damage of guest property, food-related illnesses, and company-wide complaints.

Guest accidents are, by far, the costliest claim your property will handle. A slip and fall that involves back surgery or long-term loss of a bodily function or limb can cost hundreds of thousands of dollars. If the case goes to a jury, your little investigation might save or cost the company millions. This is not an exaggeration as the examples throughout this book have illustrated. Liability, safety, and prevention of accidents are addressed elsewhere in this book, so we will focus only on the investigation here.

Triggers

Your department may not have the work force or the time to investigate every guest report that comes through. If that is the case, you need to develop triggers that automatically start an investigation. For reports involving guests, here are some examples of criteria that would trigger an investigation.

Loss or damage greater than $250
Any guest injury
Complaints that are serious, such as discrimination
Where the return is greater than the cost of the investigation (sometimes it is cheaper to pay)

Statements

We discussed gathering statements in the section entitled Preliminary Investigation. The investigator will put that statement to good use because it is unlikely that there will be an interview or further contact with the guest. The investigator can use the information in the statement and see where it differs from the verbal account given to the officer. For example, when the watch was first missing, it was worth $100. When the guest wrote the statement later, it was valued at $500. When the guest calls your claims representative, it is now worth $5,000. We use the statement as we did with interviews, but in lieu of getting to speak to the guest.

Witnesses

Witnesses are handled differently depending on whether they are guests or employees. Employee witnesses are treated as they are in a personnel investigation: Obtain and evaluate statement and interview as necessary to gain more information. Guest witnesses can be contacted after they leave, but it is not likely to be in person if they are tourists. Phone interviews do not work well for discerning the truth but are perfectly acceptable for following up to clarify what the guests wrote in their statements.

“Suspect” employees should be investigated exactly as with a personnel investigation. Remember that with a personnel investigation, the objective is to prove a policy violation.

In a guest loss, we are trying to prove that we have no responsibility for the loss. These two objectives seem to conflict because if we prove an employee was responsible, then the hotel is vicariously liable for the loss as well.

Your Risk Manager or Claims Department may not want to investigate certain incidents because they can more easily deny the claim and responsibility if there is no evidence of hotel responsibility. In the old days, Security departments would keep their investigations confidential for that very reason. That way the claims person could pick and choose the investigative reports that favored the hotel. We all know this is wrong and no longer even true. Any documentation can be called into court, if it goes that far.

ANALYSIS

As I said at the beginning of the Investigations section, investigators are the most skilled employees you have. They can and should be used for other important functions than just loss recovery.

Metrics

"Metrics" means "to measure," which is why it applies to the socket set in your toolbox as well as the measurements of your department. In fact, toolbox is a good allusion for how Security uses metrics.

Measurements of the department come from a wide variety of data sources and are used for just as many reasons. One metric you are already using is your daily labor report. This report, from the company's timekeeper, tells you how much you spent on labor, how much overtime, how many hours, and so forth. The time clock is the data source, and the report is the metric. Someone put that metric together for the managers in your company based on what metrics he or she was told you needed. You could expand that report to include other measurements if you knew how to access the data and how to create the report. You probably do not "own" time clock data, but you do own other Security data, so all we need to work on metrics is a data source and a reporting tool.

Data Sources

Let's determine the types of data sources, then what metrics we want, then how to get from A to B. However, even if we do not know what metrics we need, the sooner you start collecting data, the more data you will have to work with when you are ready.

It is the investigator's responsibility to track losses and incidents. In Chapter 1, we talked about tracking incidents so that we know where vulnerabilities are. In Chapter 2, we discussed using hot spots to deploy staff and resources. In this chapter, we will use the tracking to find trends in Internal theft and other vulnerabilities so we can use measures to reduce them.

Incident Reporting software is supposed to do much of this legwork for you, but that is not always the case. Whomever compiles your data and gives it to you in a useful form, it should include the following:

Date/Time of incident report—This is the time the incident or loss was reported to security, not when it was discovered and not when it happened.

Date/Time Range of loss—Often we do not know when a loss occurred, a property loss in a room, for example, so we have a range which is the last time the person saw it until the time they noticed it missing. Day of the week will turn out to be important later as well.

Location—We need a general location: East Tower, Restaurant Row, etc.; A named location: Room 312, Joe's Coffee Shop, etc.; and a sub-location: The bathroom, Table 15, etc. Tracking room losses requires an extra field of "floor" and/or "section."

More Data Is Better

Guest check-in/check-out date will come in handy for room losses later.

Property Description—like location, we need a category (jewelry, electronics, clothes); a general item type (ring, tablet, cash); and an exact description.

There will be other categories depending on what we are tracking.

Next, build a simple spreadsheet in Excel, or whatever you prefer (not paper) using the descriptors and fields I described above as headers for individual columns. More columns means more data and that is better. Each row of your spreadsheet is an incident. Use a separate spreadsheet for each type of incident (room losses, accidents, other losses, etc.).

Once you begin building data, like pages of data, you can start sorting it. (Your reporting software can do this generally with canned reports or may allow you to make custom reports.) But forget paper because the next step makes that impossible.

Use Excel to sort your data. You can sort by employee and see which GRA happens to be the cleaner of rooms with most losses. You can sort by date of occurrence and check-out date to see if losses occur more on check-out days or stayover days. You can also narrow down by floor or day of the week or whatever.

Analyzing the Data

There are so many things you can discover with this treasure trove of information. You may find employees that you did not suspect, or those you can rule out. You can cross-reference so that of a 10-year employee who rarely has losses, but always trains the new ones and thus, gets blamed for those thefts. You may find other problems besides employees. One specific room, which has more losses than others, might have a faulty door closure. Whether it is employees, policies, or environment, the investigator should recommend changes to prevent future incidents based on the data derived.

In one hotel, every time there was a property loss from a room, the procedure was to get a statement from the housekeeper. Over several years, the procedure started becoming less effective. It had been designed to get the report taker to interview the housekeeper and put their story in the report. ("Did you see the tablet?", "Were there any personal items in the room?", and so on.) As security officers often do, they took the path of least resistance, which was to leave a statement with the housekeeping manager with a message that said something like, “There is a tablet missing from room 312. I need a statement.”

So the Housekeeping Manager, in an effort to keep his employees employed, told the GRAs to write the following: “I did not see the item. If I do find an item, I always turn it in to Lost and Found.” The statements began to look like photocopies of each other. If the Investigators decided to interview a housekeeper about a room loss, they would get a longer version of the same diatribe: “I did not see the item. If I do find an item, I always turn it in to Lost and Found.” This went on, with few cases being solved, until a new investigator was hired that was bi-lingual. (Most of the housekeepers were Hispanic.) He began to solve cases on his first day not because everyone was stealing, but because they had useful information on the missing property but were told to keep their mouths shut—information such as, the teenager had the tablet when they left the room, or the guests had a fight the second night and the wife took everything with her. Guest-Room Attendants are not bad because of their country of origin or their proximity to a guest’s valuables. They can prove themselves to be a loyal, valuable member of the team just like any other employee if they are treated as such.

We are not looking just for employee theft. Analyzing slip and falls may lead you to the conclusion that a certain floor is just too slick. Or mopping days have more falls than other days. Or as I found, mopping days have less accidents because “wet floor” signs are out, and people are more careful.

A hotel where I worked had a waxed and highly polished concrete floor throughout much of the public areas. Close proximity to the restaurants and bars meant that a lot of food and drink was spilled on that floor and unfortunately, a few slips. On busy weekends, a guest accident could really tie things up, with traffic control, the incident report, and of course, ruining the guest’s stay. One of my colleagues came up with the idea of placing dry, cleaning towels in strategic places along that concrete walkway. Towels were behind planters, hostess podiums, and anywhere that they could be discreet, but handy.

After acquiring the towels, we had to create a culture of using them. Fortunately, the security guys had already bought in because they did not want to deal with accident reports all night. The next thing was to get every single employee in the habit of looking for spills and cleaning them immediately. Most took this on gladly. Some were called out after we showed a video of them walking right by a wet spill. Worse yet, tell them that they walked by a spill right before a guest slipped in it. Nobody wants that.

The result was a new procedure for towel stations and fewer slips. In fact, on busy nights when volume was ten times normal, we could go without any slips at all. This is Risk Management at its best.

Slip and Falls

Guest Accidents likely cost the hotel more than any other incident. We do not like our guests getting injured and ruining their stay—and they don't either. Guests may have a bad knee, poor eyesight, or are just clumsy. Even though everything seems jake when you speak with them, by the time they get home, especially when they get their hospital bill, they are likely to come to the hotel looking for some reimbursement, and then some.

It is usually the risk manager's job to work through these incidents with the guest, but they need a well-documented summary of the incident. Even a guest who gets up, brushes himself off, and insists there is no need for a fuss, can come back a year or more later and file a lawsuit against the property for causing his fall. Since I have worked for both defendant and plaintiff on these cases, I will admit that sometimes the guest's claims are legitimate and sometimes they are not. Fortunately, this is not directly your problem. Your job is to investigate the incident and get as much information to the Risk manager as possible. I dare say, most companies will take responsibility if the company was to blame, but nobody likes paying on something that was entirely the guest's fault.

The example above of the preliminary investigation is the first step in the process. The investigator then dives deeper into all of that and comes to some conclusions—not opinions. For example, the investigator will look at video of the area of a slip and fall prior to the accident. It may show the liquid had just been spilled or it may show that it was there for hours with no employees bothering to clean it or report it. The first example is good for us because we did not have "notice" of the spill so it will not be reasonable to expect us to have seen it, but in the second scenario, we bear some responsibility for not patrolling, observing, and maintaining the clean floor.

I have seen some pretty poor acting performances by persons faking accidents in an attempt to defraud the hotel. Nevertheless, the investigator leaves no stone unturned reviewing video, re-interviewing witnesses, possibly speaking with the guest again, and looking at the entire situation through their experienced eye.

CRIME ANALYSIS

It is the responsibility of the Security Director to be preventative more than reactive. Even police departments that traditionally focused on reacting to crimes and trying to catch criminals on the back end are now using crime prevention techniques to reduce the chances of a crime occurring in the first place. We already know physical prevention techniques and they are discussed throughout this book, such as layered security, preventative patrol, and behavioral analysis. Another important method that you should be using, and may already be using to some extent, is crime prevention analysis.

The concept is to use data, as we did in our Risk Assessment, to prevent crime by investigating patterns. As you analyze crime statistics, you will notice trends that suggest certain commonalities. Burglaries may occur on certain hotel floors, at certain times of the day, or by certain methods. Crime (or incident) analysis is the sorting of data to reveal patterns, exceptions, and trends. Now that we have a spreadsheet with some data, or a reporting system that provides us with presorted information, we can start to see what we have. There are many ways to look at the data and you really need to look at all of it for it to be of any use.

Location

You may start by dividing your property into general locations, such as garage, guest rooms, nightclub, and lobby. These areas are so different that there probably will not be any overlap of crime or incidents. In other words, statistics that you derive from the garage or parking area will not likely be related in any way to crime you have in guest rooms.

Once you separate these areas, you can work on data from each one separately. In each of these areas, you will want to have sublocations, or locations that are more specific. These may be floors in a garage, or quadrants in a parking lot. In the hotel, it would likely be floors. In the public areas, you have the lobby, each restaurant, bar, etc.

When you sort by these areas, you may already see patterns, such as one particular floor that has problems over another. In Valet, or the nightclub, of course, every incident is in that location, so skip this step for those specific areas. If you notice a trend or something unusual about a particular location, there must be a reason and that is what we are here to solve.

Crime Type

The next "sorting" method of analyzing crime data is by type of crime. This will show you at a glance if you have more of a problem with damaged cars in Valet, rather than property loss; or property loss in guest rooms, rather than assaults or robberies; or more fights in the nightclub than missing purses.

Time

The next sort option is date and time. Here you are looking for commonalities related to time of day, day of week, shift, etc. Perhaps most car burglaries occur between 7 p.m. and midnight. Maybe room losses usually happen during the day. Fights in the nightclub occur most often on Wednesdays. (This seems very elementary to most of you, but you need to follow the steps to ensure that you do not overlook anything. We will get further into the analysis shortly.)

Suspect

Another sorting option of our crime data is the suspect. The obvious pattern might be a housekeeper who has coincidentally cleaned all the rooms where losses occurred. Less obvious are profiles of suspects. You probably do not have suspects identified in most cases. However, in nightclub fights you should have descriptions. Do white males in their early 20s start all the fights? The same goes for losses in the kitchen. You can rule out a bunch of staff members if the suspects all had gray shirts and the kitchen staff has white shirts.

Other Sorts

If you find commonalities in your data, it will be worth it to drill down deeper into other categories. These may include specific room numbers, approximate times, etc.

Crime Triangle

Three of the categories we just talked about make up the crime triangle. This triangle is a useful illustrative way to solve and prevent crime.

The crime triangle consists of three components of a crime: location, victim, and suspect. Every crime must have a victim, one who suffers from the crime; a suspect, one who commits the crime; and a location where the crime occurred. (The location may be virtual, such as the Internet or telephone.) Take away any of the three components and there is no crime.

Suspect

The suspect leg of this triangle is traditionally the one we go for. The suspect is the bad guy, the one breaking the law, so that is generally where we concentrate our efforts of solving crimes. If a neighborhood is having a rash of car burglaries, the police try to catch the bad guy and, thus, eliminate future crimes. Of course, this is great if you can do it, but it is best to let the police do that and for us to concentrate our efforts on preventing the crime from occurring again. Catching the suspect may prevent the suspect from committing the crime again, but it is only one third of the prevention. Someone else can come along and commit the same crime, theoretically.

Without getting too far into psychology of a criminal, it is important to understand a little bit about his/her thought process. When most of us make a decision between good and bad, we use rational judgment that takes all of the factors into account: How will this affect the other person? Will I be caught? What will happen if I am caught? How would I explain that to my loved ones? And so forth. Most of us choose not to commit the crime because of the way we answered those questions. (This may explain why alcohol turns normal people into criminals.)

The criminal mind generally works a bit differently. The thief or assailant does not ask himself those questions (until afterward, maybe). He sees the immediate gratification of possessing the item, committing the violent act, or the thrill of the bad act. This makes most criminals opportunists and shortsighted thinkers. It helps us to know this because we know that if we decrease the opportunity or make it more difficult or time-consuming to commit the crime, we can prevent many of these acts.

For example, a wallet lying on a counter unattended is too tempting for someone who does not ask himself the questions. He sees an opportunity and takes it. If the owner is standing near the wallet, it becomes less of an opportunity and less tempting because the immediate gratification becomes less likely because the person may fight him. If the owner is holding her wallet, that makes it far less tempting. The gratification is now out of sight to most (unless they are a skilled snatcher and do not see the person holding it as a deterrent).

One exception to this theory is the criminal who “justifies” his actions. It should have been mine anyway; they do not deserve to have it; they can afford to lose it; she hurt me so I will hurt her; he fired me so I will show him who is boss; etc. Since we know there are criminal minds out there, and plenty of justifications, we have to limit the opportunities.

Victim

Of course, if we get rid of all the victims, we can certainly prevent crime. That is not very conducive to the hospitality business. Seriously, we can have some influence on potential victims to prevent them from becoming victims. We do this all the time by warning vehicle owners to lock their cars and not to leave valuables inside, providing awareness training, posting signs warning patrons, etc.

Anything you can do to get hotel guests out of the "tourist/victim" mentality and make them more self-aware is a way to prevent crime. We want our guests to have a worry-free stay in our establishment, so we must find a reasonable balance between paradise and prison.

Location

Naturally, if you change or eliminate a location of a crime, it will not happen again—at least not there. This is also a common prevention technique we use. If crimes are happening in a certain area, we beef up our patrol, install cameras and locks, etc. Consider these measures in your hotel.

The crime triangle is something you were already using, and maybe did not realize it. However, when you approach crime prevention using the triangle model, you will focus on all three legs, rather than just one. This gives you three times the opportunity to prevent the crime. As you review crime trends from the data you compiled, determine which leg provides the commonality. Location is easy. More car burglaries are occurring on the fifth floor of the garage or door pushers keep hitting the same room, which has a faulty closure. These are easy crime trends to address.

Sometimes the trend is not location, but suspect. For example, if you have a problem with graffiti, it may happen all over the property, but you can develop a profile of the suspect easily. It may be video, or you may know what gang the suspect comes from. Then your prevention step might be to identify those persons and watch them or exclude them.

Finally, the data may show that the commonality is the victim. The obvious example would be little old ladies who keep getting robbed of their purses. You may want to put more resources on watching little old ladies with purses, warning people not to carry cash in their purse, or providing awareness training.

Off-Property Incidents

In Chapter 1, we mentioned the importance of gathering outside data for performing the Risk Assessment. Investigators or analysts are usually the likely persons to track this activity. Besides assessing risk, we need to know what is happening at other hotels (or similar properties) and at neighboring businesses and streets. The criminal activity in our neighborhood has many effects on us. It makes or breaks our reputation, makes our guests and employees feel threatened, and determines what types of security measures we will take.

Street crime near your property may prompt you to install lighting, locked gates, fenced parking, etc. Other hotels with a propensity for crime may encourage you to take preventative steps to avoid those crimes on your property. Gang activity in your neighborhood will decide whether you have dress codes, controlled entry, or even armed security.

For all these reasons, track activity on a spreadsheet just as you do for internal incidents. List the major incidents specifically, such as with a news clipping, and other incidents by category and location. If applicable, list the security measures you took to reduce the chance of those crimes happening.

Reacting to the Data

Measuring the incidents we have, sorting the data, and analyzing it not only provides nice reports for the boss, but also can help solve the problems, thereby protecting the assets even better. The traditional method was to go after the bad guy. But the crime triangle shows us that the bad guy is only a third of the problem and not necessarily the easiest side of the triangle to remove. Remember that our job is to protect the assets. The most efficient way to do that is through prevention. Arresting people, or even firing people, does not always prevent the loss.

So, what else can our crime analysts recommend to prevent future crimes or losses? The answer is in the data. Look at the information you have and determine the most efficient method of preventing it from happening again. Lighting, cameras, locks, patrol, training, awareness, and special operations are just a few of the tools at our disposal, and the solution should be obvious in the crime data.

SPECIAL OPERATIONS

After performing a crime analysis or beginning a specific investigation, it may be determined that the suspect leg of the triangle is the one we need to remove. As long as we admit that this will not be preventative in nature and will likely cost more, it is perfectly justifiable to go after the suspect, especially if it is an employee. These temporary operations are designed specifically to target one suspect or a group of suspects. Operations include undercover officers, outside agencies, or covert cameras. They may include targeted area patrols, new procedures, or training.

Undercover Operations

Undercover operations encompass a wide variety of plainclothes, covert, or discreet investigations depending on the objective. I find that either Security Departments do not use them enough or they use them too much. The advantage of a discreet operation is that it addresses those offenders who are privy to the visible security measures. Disadvantages are that they are not very preventative in nature—more reactionary—and often take resources away from other necessary areas.

Outside Agencies

It may be appropriate at times to ask local law enforcement agencies to conduct a special operation on your property. Naturally, this method can only be used for suspected criminal activity. If your problem is a policy violation or anything less than criminal, the police cannot be of much help. However, they may be very interested in working a known problem with prostitution, drug dealing, or fraud.

If police detectives are assigned to work your property, you will be placed in a supportive role. You should provide whatever information they need and whatever technical support you can. See the section on Prostitution in this chapter. Suggestions for law enforcement investigations include prostitution, organized crime, drug sales, car burglaries, etc.

Private Outside Agencies

Other loss investigations should not be handled internally. A complicated internal fraud case is an example of an investigation that requires a great deal of resources, an unknown undercover employee, and a perspective that is strictly unbiased. Even if you are confident in the ability of your staff to perform this operation, and to do so without favor, remember that perception is reality. The outcome may be questioned morally or even legally if there is even a hint that your relationship with co-workers affected the investigation.

There are many very qualified private investigators to use for such an investigation. If you do not know someone who can give you a personal recommendation, go through your local security association or police liaison. Your company law firm may have a reliable company that they have used in the past. This is not a job to be chosen from an Internet search.

Like the police, you will have to hand the entire matter over to this outside person. As with any secret, the more people you tell, the less likely it will be a secret. Every executive wants to know and thinks he has a reason to know, but it is better if only one person knows.

Use the guidelines set out in the Personnel Investigations section of this chapter in defining your objective, what the expected outcome will be, if there will be charges filed, a term, etc. Suggested uses for an outside employee investigation include fraud in the Accounting Department, bartenders stealing, Receiving Department losses, nightclub doorpersons stealing, employee drug use, etc.

In-House Operations

Integrity Checks

There are three reasons we do Integrity Checks on our employees.

1. To solve a trend of losses.
2. To let employees know we are inspecting what we expect.
3. To satisfy our own internal audit procedures.

An integrity check is an audit of employees at a certain time, a specific place, to ensure policies are being followed and behavior is appropriate. There are several ways we check the integrity of our employees in a hotel. These checks are also known as "setups" or "stings." Missing property from a room is an age-old complaint that is caused by the following. It is rarely an actual theft.

1. Guest Error—In my experience, most missing property cases are the fault of the guest. They misplace their property and assume it was stolen. Often, it was simply left at home, or the teenage son took it, or whatever. Unfortunately, guests do not generally call you back and admit their mistake. Sometimes they do, which is great, but otherwise, we are left questioning whether we had an actual theft or not.
2. Door Pusher—As you know, door pushers are those that troll the halls looking for doors left ajar. It is amazing to me how many fellow guests take advantage of an open door as they pass it on the way to their own room.
3. Employee Theft—Yes, the GRA can be a suspect, anyone with access to a room is a suspect: Security, Bell Persons, and facilities.

The most difficult part of doing integrity checks is deciding when, where, and how you will do them. Remember that we have learned the need to start with an objective to answer the when, where, and how. Unless we are doing random audits to satisfy our protocols, we need to gather data to form our objective. Earlier in the chapter, I explained how to track room losses to find trends and solve cases. Without this method of narrowing down a room or person to target, we might just be spinning our wheels.

If you have a room loss, do not automatically assume, or accuse the maid of being guilty. In a common hotel, guest-room attendants are long-term employees who have built a personal reputation. They likely do not steal as it is not worth it, and they feel some loyalty to management and their guests. Let's face it, they are not in it for the money or glory. I am generalizing of course, but I think this covers the vast majority.

Some hotels, especially in difficult labor markets, hire temps or J-1 visa holders. Neither of these groups are long-term employees and they usually do not go through the same background check, have references, a good work history, etc. Again, there are exceptions, but this covers most of them. (J-1 visa holders are usually students from foreign countries who come to the US to gain work experience for a few weeks or months.)

The other source of GRAs is the contract companies. These companies are like temp agencies or guard companies. There is a reason the individuals did not hire directly with your hotel and it is usually not a good one. Of course, many are great, honest employees but we are weighing risk here.

The second variable to look at is location. What I have done in the past (and this is covered in more detail later) is to keep a spreadsheet of room losses. This matrix will give you some likely rooms or GRAs to target in your integrity check.

The Preliminaries

Remember we need to know our objective before setting up these procedures. The procedures will vary greatly depending on whether you are looking for a criminal prosecution as compared to a policy violation or even a deterrent value. No matter which method you decide, document the way you do it and the locations and times. This needs to be consistent to be effective.

I gave you three possible objectives in the previous paragraph. As for aiming for a criminal prosecution, I do not recommend it. The burden of proof and the elements you need to prove a burglary or theft charge are difficult and complicated to document. For burglary, you would have to prove the employee entered the room with the intent to steal, or that they broke into the room, or other elements not likely to apply. For theft, you would have to prove the employee intended to take it home, which means you would have to track the item all the way to end of shift and out the door. It is easier to prove a policy violation and you will not have to involve the police, the courts, or use time and resources preparing a case.

Review this process with your counsel and your HR folks to make sure there are no legal issues preventing it. If your GRAs have a union, this will get grieved up and down. That is why you need to be honest, transparent, and consistent with your methods. Even if there is no union, you have privacy issues, accusations of discrimination and other legal hurdles that might make these folks uncomfortable.

Before starting, make sure the department has published the policies on entering and servicing rooms (what not to touch, etc.) and Lost and Found procedures. For example, if you catch an employee putting a necklace in her pocket, she is likely to say she was going to turn it in at end of shift. Hopefully you do not allow that, and you can terminate her for violating procedures.

The Setup

In an integrity check for hotel rooms, we will rent a room, make it look occupied by a guest and put some property that might entice someone to steal it. Does someone want to call this entrapment? Remember we are not seeking criminal prosecution, so it does not apply.

If you get past all that, you need to set up your room. First, you need to rent a room and possibly a second room. Do not use your key to just takeover a room. Housekeeping gets a rooming report daily and you want to be on it. I would advise not telling anyone in management either. Though they may be on your side and they may have good intentions, people just cannot keep a secret. So, go through the motions of renting the room in a name not known in the hotel.

Part of your setup includes hidden video (which means you get to buy some cool gadgets). You will need to watch it live (especially if you want to recover your stuff). That is generally done from a nearby room. Or you may have a room, like a closet or something that you can use. Not a place where Housekeeping has access. In the old days we had these huge cameras with wires running through the walls. Fortunately, you can now use wireless devices that are very small. The trick is to find one that transmits the picture, runs on battery, and has a long battery life. Your lawyer may bring up the expectation of privacy. Good question. First of all, do not allow a guest or anyone else in the room. Second, be sure your Housekeeping policies prohibit taking breaks in guest rooms, including the restroom. Third, cameras can be positioned so that property is in the image, but the housekeeper is not. That way, if he or she starts adjusting their underwear in the room, there will be nothing inappropriate.

Once you have your video production ready to go—and after all, that is the fun part—you will need some bait. I think most of us would tend to go to our Lost and Found stash and use some of that merchandise. Two problems with that: One is that it is mostly junk that does not match. You need a suitcase full of stuff that belongs to a male or female or a couple. Second, the GRA may recognize things from Lost and Found. However, you want to come up with it, I would get a suitcase, pants shirt, underwear, etc. For the valuables, go back to spreadsheet and see what tends to go missing from rooms. Tablets? Jewelry? Cash? Drugs? Etc.

Now Some Warnings

Check your policy for items on the bed. Some hotels do not allow the GRAs to remove items from the bed. It works either way, but you need to know.

Do not leave a bottle of opioids, for example, to be stolen. This is a liability you do not want. One investigator told me that he put Tylenol in the bottle and glued the lid closed. Temptation is for them to take a few pills that will not be noticed immediately. Let them take the entire bottle or leave it.

Remember that a stayover means the guest is coming back. Are those the rooms that get hit at your place? Or is it the check-outs where items are mistakenly left behind.

The Sting

So, you are on your first stake-out and Mary comes in, cleans the room, and leaves the dirty sheets on the floor. Get to know your housekeeping procedures because there may be several people that come in that room. A houseman may be assigned to empty trash and pickup dirty linen. An inspector may be the one who comes in and checks to make sure the room was cleaned properly. There may be Engineers (facilities folks) that are called in to change a light bulb or fix frayed carpet. This is fine but you need to know about it.

Well, it turns out that Ernie the Engineer has found a bottle of pills behind the toilet he was fixing. (Not even part of your sting) and he puts them in his pocket and leaves the room. This is an unexpected bonus. Since it is drugs, you may want to call the police. Do not try to do their case for them. Focus your efforts on the policy violation.

More Warnings

Decide what you will do if: (1) Ernie refuses to go to the office with you, (2) Ernie gave the pills to another worker, (3) Ernie is a union employee, and (4) Ernie says he consumed the pills for his bad back.

After reading this, you are probably thinking that integrity checks are not worth the trouble. I still disagree. The best value they have is the deterrence factor. No matter what happens with your suspect employee, word will get out. Every employee will know that you use covert cameras to keep them honest and they will not know when and where. This makes thieves think twice. Another silver lining is the policy violation. As we discussed earlier in the chapter, the intent and the evidence threshold are much lower for a termination. You can still get rid of internal thieves, keep your employees honest, and protect your hotel's reputation by doing these integrity checks.

Integrity Checks can be accomplished in this way in other areas as well. Liquor storage, retail, and anything involving merchandise are great for these stings. Be careful with offices as they may have an expectation of privacy. If you are looking for other shenanigans such as sex in a closet, also be careful of the privacy aspect. A camera monitoring the outside of the room may be sufficient.

Covert Cameras

Covert cameras are those that are hidden from view or disguised as something else. Before you even think about using hidden cameras, check with your legal counsel on issues such as expectation of privacy and wire-tapping laws. There is no specific law about where to put cameras. The precedents are set in federal and state case law about what is reasonable. We also follow different rules than the police do because we are private. There are now very specific laws in each state about audio recording. These laws come from older wire-tapping laws. Some states are keeping up with technology (to include video) and others are not. So, your state might forbid recording an audio conversation and allow (by lack of any laws against it) video recording.

> A New York jury awarded a man $3 million after he sued his employer for discrimination. The man had made several complaints regarding ethnic slurs from his co-workers. There was no apparent investigation of the slurs, but a camera was placed in the man's work area to watch him, presumably to retaliate for his complaints.
>
> Cameras are a good way to document misconduct or criminal activity but should never be used in this manner. The Security Director or Human Resources Director should authorize such use of cameras to ensure that employees are investigated fairly and that labor laws are not violated.

To keep you out of trouble, here are some rules that should cover you in most states. Do not place a video camera in a place where someone would expect to have privacy. This includes bathrooms and dressing rooms, but also may include a private office or even a storeroom. Make sure you have a documentable reason why you need a hidden camera there. Reasons include a rash of thefts from the area, reports of misconduct, such as sexual activity or sleeping, and suspicion of fraud on a computer. Do not place a hidden camera in an occupied guest room. Consider a general policy about video surveillance for all employees. Do not audio record someone in secret.

Some great ideas for camera placement have been used in hotels by clever investigators. Your networking with other directors and investigators will give you good ideas and save you from duplicating mistakes.

There are numerous camera options available these days due to their smaller size. Cameras can be secreted in almost anything and if you have a technician available with a little imagination, she can probably put a camera in just about anything.

Suggested uses for in-house operations include losses from guest rooms, storerooms, valet vehicles, and lockers; employee vandalism; safety violations; and harassment.

Bag Checks

The unfortunate fact is employees walk off your property with company merchandise every day. Whether it is shampoo, towels, and soap, or alarm clocks and hair dryers, or even alcohol and guest property—chances are there are some thieves among us. A simple deterrent to this is to do bag checks daily at the end of shift or at least randomly.

Like shoplifting, it is difficult to effectively stop internal theft. You can ignore it and take the loss, or you can do some things to cut it down as much as possible. Unfortunately, if you ask your controller or purchasing director what the "shrink" amount at your hotel is, they likely do not know. Just like vegetable oil in the kitchen, these household items that are stolen are included in the amenities and the cost of doing business. Alarm clocks and toilet paper are inventoried in bulk and likely not accounted individually. Besides, much of this merchandise is taken by guests. So I might have just talked you out of it.

However, what if toilet paper leads to lobsters or alcohol or drugs found in a room. For the sake of your guests, your reputation, and the bottom line, you need to take some reasonable steps to stem this tide. Some studies put employee theft at six times that of guest theft. We both know that is because we do not put as much focus on internal theft. So let's look at some basic things you should probably do at a minimum.

The ideal policy would be to have a security officer inspecting every employee who leaves the employee areas (back of the house). This is often considered not worth the labor required, or not practical due to the layout of the basement or employee area. Twenty-four-hour inspection posts are certainly expensive, so it may be worth it to do random bag checks.

Bag checks are simple and can take less than 30 minutes. Station two officers at the employee exit and inspect every purse, backpack, and duffle bag that comes through. Do not target housekeepers only. That begins to look discriminatory, especially because there is plenty of theft from other departments. Require every employee to go through this process to be fair. Make sure the second officer is watching for employees who see the inspection site and head back to their lockers.

A hotel where I worked had an employee inspection post that ran 24/7 for many years. When we went through the recession, we decided to cut this post to devote our limited manpower to guest safety. Soon, I instituted random inspections. On the first day, the very first employee who walked past the inspection area was a housekeeper with an alarm clock in her purse. Several more were seen turning around and heading back to their work area.

Investigators can assist with bag checks and take the opportunity to specifically watch certain employees who appear in their metrics more than others do. They also may want to set up an integrity check of storage areas and use the bag check to check for stolen products.

Make sure your company has a policy about employees being subject to search. Signage is a good reminder.

Many properties have electronic access control which can help compel employees to the entrances and exits that are monitored. If you do not have this tool, at least use policies to steer employees toward one exit so they do not know when the exits will be monitored. Video is also a given for back of the house areas, although it provides little deterrent unless it is monitored and acted upon.

DRUG TESTING

Before you can test for drugs and alcohol, you better have a policy to guide you. The policy is likely written by your HR so if you don't have one or don't know it, get with them. Here are some things to think about so it is a little more complicated.

According to studies published on the Internet, the hospitality industry employs the largest number of workers with substance abuse problems. That is likely due to the presence of alcohol as part of the job duties in hotels, restaurants, and bars. Alcohol is just one part of a nationwide drug problem that is woven into the fabric of our workforce. Whatever the statistics on substance use or your own personal feelings, we can probably all agree that it has no place at work. Besides, if the company has a policy against it, it is your job to enforce it.

Most drugs take effect on the mind and body within about 30 minutes. Their effects can last up to four hours in most cases. (That means someone who is under the influence in the second half of his or her shift most likely consumed the drug while working.) Testing methods include urine, blood, and saliva. (Hair testing does not work to see immediate effects so it is used for pre-employment screening. Sweat, or patch, testing is used to check for usage over a long period.)

Marijuana laws are evolving to make the drug, and the tolerance of it, more prevalent. As I write this, the Federal Government still considers the substance to be in Schedule I which includes drugs that have no medical use. In other words, it is still illegal according to the federal government. Many states have chosen to defy that law and pass their own laws legalizing marijuana with various restrictions. There are many legal and political arguments on both sides, which I will try to avoid here. However, these decisions do affect us directly.

For example, an employee who uses marijuana off duty on Saturday and is involved in an accident on Tuesday, he will likely test positive for Cannabis. The company needs to decide how they will deal with this. Is pot smoking going to be against policy even at home on days off? Many companies struggle with this and have tossed their hands up and softened their policies altogether. This is probably not your decision. You are the enforcer in these cases.

For some time, a few years ago, the Occupational Safety and Health Administration gave an opinion that confused everyone about drug testing policies. There was a statement issued that considered pre-employment testing as "random" and that random tests were not permissible. They clarified their position in 2018 that drug testing was allowed under the following conditions.

Random

Companies generally do drug testing in four different circumstances: pre-employment, post-accident, random, and cause. I will assume that you have little to do with the pre-employment screening, so we will discuss the other three, which are almost identical processes. First, a brief discussion about drugs.

For our purposes, we can classify mind-influencing or psychoactive drugs as either stimulants or depressants. (This is over-simplified for illustration only.) These "controlled substances" are alcohol, marijuana, prescription drugs, and street drugs. Each of these substances affects judgment and physical skills and, therefore, can cause accidents and poor work performance and place a company in a bad light.

Your HR professionals, legal counsel, and company medical provider should decide testing methods and policies. Some bargaining agreements have special stipulations about testing methods that must be followed. Whatever your procedures are, these are my recommendations and you can adapt them to meet your requirements.

Random Testing

Most companies do not allow for random testing (except for regulated employees like bus drivers, airline pilots, and sports figures). The accusations of discrimination and favoritism are too difficult to defend for normal workers and it is difficult to administer. If you do have random testing, it is likely that Security will not be involved, but if you are, follow the procedures in the next section.

Post-accident

Almost every company requires a drug test following an employee accident. Your company will have to decide if this is done for every reported accident, those that just claim injuries, or those that require medical treatment. I would suggest any accident where an injury is claimed gets a drug test. Before any testing is done, the employee should be required to sign a policy statement with a witness. The policy should state three things:

1. The company requires the test and refusal to take it will result in termination.
2. If the test comes back positive or has to be sent for further testing, the employee will be on investigative suspension.
3. If the test is positive or requires further testing, the employee will not be permitted to drive home.

To save time and money, I recommend using a swab test that can be given by Security. These tests are a few dollars per use, test for a wide variety of drugs, and give immediate results. If this test is negative, it is finished. If the swab were positive, I would have it corroborated by a professional lab. Do not rely on this test for a determination of substance abuse. It is presumptive only. Swab tests also do not have thresholds, which means someone on a legal prescription dose of valium would come back as positive.

They make swab tests for alcohol or you can use a breathalyzer, which provides a blood/alcohol percentage. This may be important to your HR Department because it is written into most labor agreements.

Lab or clinic testing should be of the type recommended by your medical provider. They may want to do urine, blood, or both. Urine testing means the employee has to pee in a cup. The clinic will tell you all sorts of stories about how these are defeated by guilty employees, but the clinic personnel know how to spot deceptive tricks. The blood method involves drawing a blood sample. Different substances stay in the urine and in the blood for various durations and at varying levels. The comparison of blood and urine helps the lab technician decide the level of effect that the employee has. If you have a local medical clinic that is available 24 hours, you will have to have someone drive the employee to the clinic for testing. Most clinics will provide preliminary results immediately. If there is a suspected positive, they will send the sample to a lab and results may take one to three days.

If prescription drugs are indicated in a test, the lab will usually contact the employee to justify these medications and provide prescriptions. The level in the body must meet the amount prescribed. Most lawyers will not allow a termination for prescription drug use.

Cause Testing

Testing an employee for "reasonable cause" is quite a bit more subjective than post-accident. The justification is not as clear, but with the right policies, we can make it simple. You should start with a policy that allows for drug testing if there is reasonable suspicion that an employee is under the influence. Then require a manager to have that reasonable suspicion. No special training is involved if you use the "reasonable person" test. Assuming your managers are reasonable, they know what behavior is unusual or possibly related to substance abuse. To avoid accusations of targeting, require the department manager or supervisor to get a second opinion from the Security Supervisor. The two supervisors should be able to agree that they smell alcohol, note strange behavior, hear slurred speech, and see dilated or constricted pupils or a staggering walk.

The testing procedure after that point is the same as for post-accident. Fortunately, the swab testing is noninvasive and does not take the employee off the job very long if it is negative.

ABANDONED LUGGAGE

A Security Department could drive itself crazy if it overreacted to every suspicious bag. To avoid the anxiety and work force drain that these incidents can cause in a post 9/11 world, take these basic steps.

Risk Assessment

In your initial Risk Assessment, you should have determined your likelihood for a terrorist attack or bombing. A hotel in Islamabad has a much different expectation and reaction to an abandoned bag than one in Billings, Montana. In Israel, for example, every citizen notices suspicious packages and they are programed to immediately clear the area and call the authorities. You will adjust your response accordingly, but the rest of this section outlines reasonable steps for most U.S. hotels.

Back Track

The more people you have watching for suspicious activity, the better. This was explained in Chapter 2. The sooner a suspicious item is found, the easier it is to find its owner or who left it, and what their intent is. First, make sure employees are watching for guests leaving their items unattended. Forgetfulness is very common for people on holiday, so reminding them not only protects them from theft, but also the hotel from a long ordeal. Second, check with employees or even guests in the area to see if anyone saw who left the item. Third, look for clues on the bag before touching it: nametag, plane tag, or any identifying marks. These can be checked through the Front Desk. Fourth, if necessary, look at video. If you have adequate camera coverage, you should be able to see who left it and whether it was an accident. If you do not have coverage of that area, you may at least have coverage of the person bringing it in the front door or out of the elevator.

Internal Procedures

We have learned from terrorist history that there is usually a dry run and surveillance before an actual incident. A dummy bag may be left and then the action taken may be observed. A bomber who is leaving a bag obviously wants to get far enough away to be protected and avoid capture or he would just detonate while he is holding it. Following this logic, it is best to have a quick, efficient procedure for dealing with unattended bags. Besides the identification process described previously, provide officers with a basic bomb awareness class. This will help them notice the obvious signs of a bomb such as smell, stained fabric, protruding wires, etc. Train security officers to remove the item immediately—after a cursory check—and take it to an isolated area.

Official Response

If your bag or package has made it this far in the process, you have a genuine ordeal on your hands. Your likely next step is to call the police. By the way, this should not be the first time you discuss this scenario with police. Find out in advance how they want these situations handled and what their response will be. It will likely be to send a patrol officer who will make his own assessment. He will call a supervisor who will make her assessment and call the fire department or bomb squad. I guarantee none of them wants to err on the side of being blown up, so they will always take it to the next level. By this time, the area will be evacuated for hundreds of yards and your business will be closed during the investigation.

Large hotels such as those in Las Vegas and New York that consider themselves likely terrorist targets find it is worth the extra expense to conduct their own investigation prior to calling law enforcement. Shutting down a hotel in Las Vegas for two hours not only causes hundreds of thousands of dollars, but it will make world headlines. By that time, bomb or not, you have a PR nightmare. The expense mentioned involves proprietary bomb dogs, electronic sniffers, and x-ray equipment. These are costly items, but when placed against the costs mentioned, they provide a good return on investment.

(See Chapter 7 for more on bomb threats.)

INTERNAL CRIME

It is said that while you are trying to prevent one thief from entering your front door, there are six leaving out the back door. That is not a statistic on doors, but on internal theft and fraud.

We prevent and detect internal crime a few ways. First is patrol, which is discussed in Chapter 5 and in this chapter. Regular, uniformed patrol helps prevent some general theft but rarely catches a thief in the act. Second is internal audit. Internal audit is generally an Accounting or other oversight body's function and not ours, but we will talk about it as an overview. Third is the Security audit. This is not to be confused with the special operations discussed earlier in this chapter. I will explain the difference shortly.

Employee Crime Stats

75% of employees steal once—50% of those steal again
20% of revenue is lost to employee theft
38% of shrinkage is employee theft
Workers spend an average of 7 hours per week goofing off
1 in 6 workers drink or use drugs at work
50% feel one gets ahead based on politics, not hard work
25% expect to compromise their beliefs to get ahead on the job
Only 20% are "very satisfied" with jobs

Internal Audit

Let's face it, a uniformed security officer (or even an undercover one) has no chance of detecting an accountant who is transferring money to his own account, or a department head who commits payroll fraud. This is done through checks and balances performed by the company. In fact, new accounting regulations enacted after Enron and other scandals now require outside oversight in most businesses. So, sometimes we see independent accounting firms going through the books. Frankly, these people are looking for major book juggling and are not likely to catch a kickback on a mattress.

However, accountants are on the same side as Security, and we are all trying to protect the assets. Rather than work independently of them, we should work as partners. This is a relationship and a process you will need to develop through your general manager if you have not already done so. Your Auditing Department (accounting, compliance, whatever you call it) is auditing all day every day. This is a routine designed to catch and fix mistakes, prepare reports for the boss, and generate tax reports. These auditors may not be looking for fraud and might not even notice it unless someone tells them what to look for. In the payroll fraud example below, a fictitious employee is created and paid. An auditor is looking to see that hours on the check match the time clock, that the amount of the check is correct, and that the proper department was billed. If you ask them to look for duplicate addresses on checks, employees who always have the same hours, or checks that are always mailed (to name a few), they could alert you to these exceptions and you would do a follow-up audit. More on this later.

Security Audits

Security has the unique ability to watch employees. Observing an employee perform his job is the only way to prove he is stealing. Accounting or their boss may suspect theft, but the only way to catch it is to see it. An investigator performs an audit by watching an employee for a certain period and observing that procedures are followed and that the transactions are accurate. Procedures are developed to prevent loss. Examples of procedures are counting out change twice to a customer, closing a cash drawer between transactions, and checking ID on credit transactions.

When procedures are not followed, the employee will make a mistake, be taken as a victim, or commit a theft. Unfortunately, the chances of catching a thief in a one-hour audit are slim, but catching the procedure violations is common. Correcting the procedure violations will prevent mistakes, prevent robberies and thefts, and let the employee know he is being watched.

Establish a procedure with each department (not just cash handlers) so you can perform effective audits. You will need their procedure manual, schedules, and what they want audited. (You can audit smiles, uniform appearance, and time of transactions also). Once you have this information, set up a form or medium where you can get the audit information back to the department for follow-up. Of course, if you do catch a theft live on video, you will need a predetermined procedure for pulling the offending employee and conducting an investigation.

Types of Audits

Regulatory—These are not common in most hotels, but if you have departments that have to conform to certain governmental regulations, you will need to audit them to ensure they are following those regulations.

Performance—A performance audit is designed to evaluate employees doing their job. The topic may be guest service, number of guests served per hour, or duration of breaks.

Integrity—This audit is the type described previously to check for procedures that prevent loss.

Guest service—Most hotels have specific guest service policies, such as eye contact, smile and greet, providing directions, offering assistance, etc. Video audits are the best way of evaluating compliance with these policies.

Performing Audits

The first and best way to decide who gets audited is based on tips. Tips may come anonymously or they may come from a manager who suspects misconduct. They also may come from internal audit or some data where a strange pattern or exception has been identified. In the absence of any suspicions, the next way is to perform audits randomly. You may already decide that you will do one audit per week for each department. Then try to hit different employees on all shifts and in all areas. You cannot be truly random, but avoid picking on one department, gender, race, or union.

Most audits can be performed in about an hour unless there is a specific reason for going longer. If you are looking for specific types of transactions, frequency of breaks, or opening and closing procedures, you will need to adjust duration accordingly.

Next, we will review some common areas of theft and fraud that you can audit or at least be aware.

More internal (and external) theft can be prevented by strong controls and procedures rather than security investigations. There are two important components to a strong internal controls program. First is developing the proper controls. There are industry practices to follow for each job type. For example, cashiers are trained to follow several routine procedures, such as counting out change twice, checking counterfeit bills, and how money is placed in the till. If you have departments not following these procedures, suggest them to the department head. The manager will save money that is lost through theft and errors and your internal crime will go down. Second is the enforcement of the developed controls. Employees need to be audited (watched) regularly and their violations addressed. Addressing procedure violations tells the employee that he is being watched and that if he is testing us, we are going to catch him. Do not hesitate to modify controls that are lacking or missing. Better to fill the hole late than not at all.

Fraud Detection

Tips from employees (26%)
By accident (19%)
Internal audit (19%)
Internal controls (15%)
External audit (11%)
Tips from customer (9%)
Tips from vendor (5%)

These stats lead us to several solutions and one conclusion: Most initial detection of fraud comes from tips. Reduce "accidental" discoveries by increasing intentional discoveries. You need an anonymous tip line. You need to develop management communication channels (listen to employees). You need to develop an informant program. If you can, reward tipsters. Follow up with informant with results from tips. Maintain regular and consistent controls. Review controls based on prior incidents, including other hotels. When in doubt, check it out. If it just doesn't look right, it probably is not.

Your Accounting Department or whomever does your internal auditing will help with enforcing these controls and suggesting others.

ACCOUNTING

Payroll Scams

Many large businesses are victims of payroll scams. There are several variations on this, but the most lucrative is to create a fictitious employee. The department head or manager fills out the paperwork to hire an employee who does not exist (or it could be a friend or relative who does not work there). Once the employee is in the system, they clock him in and out every day and have the check mailed somewhere. If this sounds easy to do, think of the controls you can establish to prevent it. Another department (like HR) should meet and enter the employee in the system (can an HR clerk pull off this scam?), have checks picked up in person from another department, random checks of employee time record and duties performed, and camera on the time clock. Other variations of payroll scams are real employees who clock in and out, but do not work, managers who manipulate time records and take a cut of the extra money, employees clocking each other in and out or using job codes with higher pay (if you have an automated system).

Collusion

The most common form of internal theft is where two people from different departments work together to steal. Since a basic control in any money-handling operation is to have two signatures or verifiers of funds, both of those verifiers working together defeats the control. This is common in casinos, but also occurs in any business between employees of one department, employees of opposing departments, and manager and employee. The best control for this is to have a third verifier. If that is not possible, use cameras. In accounting, a common collusion is between a purchaser and an accounts payable clerk (or similar relationship). One buys the product and the other pays for it. Use your imagination: If you buy fruit for the Food Department, how hard would it be to buy a pallet of oranges from yourself and have your friend in accounts payable pay you for that pallet? He could send the check to your cousin's house payable to Darrell Clifton Produce. This is why you need verifiers, such as the receiving clerk who receives the shipment and verifies all the information on the invoice before it is paid.

Credit Card Fraud

The police have a saying: No victim no crime. If no one suffers a loss or wants to claim a loss, there is no point in wasting time on it. In an almost perfect world, when someone used your credit card (or number) to make a purchase, it would be fraud (obtaining money or property under false pretenses). And you would be the victim. You would file a report with police and if they captured the suspect, you would want him/her prosecuted. Unfortunately, for us crimefighters, we are in a credit card world, and they have eliminated the victim. If you have ever been a "victim" of Credit card fraud, you know that you call your bank, they issue you a new card and they reverse the fraudulent charges. You are out nothing. If you go down to the police station to file a report, they will remind you that you have suffered no loss so "no victim no crime." Being a good Samaritan, you call the credit card company, and you tell them that you are pretty sure the card number was stolen by an employee at the hotel, and they say, why thank you for calling. We will turn this over to our crack investigators who will recover losses and see justice served.

That last part was not exactly true. Credit card companies do not normally investigate these losses. Presumably, it is because of the sheer numbers, but when I called once (with the police in my office) regarding $30,000 in charges on one credit card, they still refused to cooperate with anything criminal.

As unsatisfying as this all is, we still need to protect our guests and our reputation by preventing and solving these frauds whenever we can. You may be surprised to learn that the credit card industry regulates merchants well. Requirements like obtaining signatures and masking card numbers are established by the Payment Card Industry (PCI). These are not laws, but requirements set forth by Visa, MasterCard, American Express, and others on businesses as a condition of accepting their cards for payment. They are very strict now and if you have not heard of PCI, go to your Controller's office and say, "What in the heck is PCI?" and watch them all jump out the windows. I exaggerate, but only about the windows—they are locked, right? Up until about 10 years ago, any busboy or guest could go through your trash and pull up a receipt containing credit card numbers. This is no longer the case. In fact, your credit card receipts now have most of the credit card number masked and it must be masked from the time it enters your system until all electronic or paper traces of it are destroyed. However, there is likely someone in your business (probably an Accounts Receivable clerk) who has access to these numbers. If so, this type of theft is hard to prevent. Make sure PCI is followed strictly in your facility.

It does not hurt to track down fraud where it is occurring at your place. Even if there is no action by police or credit companies you can still keep your workplace clean. There is more information on specific scams in Food, beverage, and Retail sections.

Identity Theft

Similar to credit card fraud, a lot of unprotected personal data of customers are floating around your Accounting Department. Several people can access names with addresses and other ID information. Are you doing background checks on every employee?

Charge-Offs

Another function of Accounts Receivable is collecting on bills. Denied credit cards, under payments, room damage, and normal bills for goods and services go through this department. Once again, use your imagination to figure out ways to steal if you are an A/R clerk making $12 an hour. Pay me a little extra and I won't report this delinquent bill to the credit card company. Send the money to my house and I will make this bill go away. Send a mattress to my house and just add 1% to our bill. Nobody would ever know. Controls like oversight and verification are keys here.

Fake Vendors

Just like payroll, it is very easy to set up a fake vendor and pay yourself for services not performed. For example, take window washers. How would an auditor know whether we actually had a vendor washing the windows every month?

CASHIERS

Voids

A very common source of extra income for cashiers is a false void or manipulation of voids. The oldest trick in the book is to sell something, collect the cash, void the transaction, and pocket the money. Most departments will require a supervisor approval for voids, but in the interest of guest service, they are sometimes approved after the customer has left.

Returns

Another old trick is a false return. A cashier grabs an item from stock, scans it as being returned, puts it back in stock, and pockets the money. Sometimes these require approval and sometimes not. Patterns and trends should be watched, and audits may catch returns and voids.

Coupon

A cashier obtains a coupon and applies it to a transaction after the customer pays full price. The cashier pockets the difference.

RESTAURANTS

Besides the common credit card thefts and false voids mentioned in the Retail section of this chapter, there are some losses unique to restaurants. Almost every food server in the world takes the guest's credit card to the back room to process the payment. That food server has temporary possession of the credit card number, the security code from the back, and even the zip code from the customer's driver's license used to verify many credit card thefts. Unfortunately, the guest does not notice the scam until he gets his statement. The credit card company will rarely investigate these crimes and the hotel will never know about it.

Even with PCI rules (credit card company compliance) protecting credit card numbers left around on receipts, technology has made it easier for nefarious frontline employees to obtain credit information. Magnetic and RF card readers can be attached to cell phones or other pocket-sized devices on a food server. Imagine a waiter swiping the customer card on his iPhone on the way to the cashier. How would anyone know? Few controls will mitigate this type of crime. One option is to limit cell phones and other devices while at work. Otherwise, you will have to wait for a report from the guest or possibly the card company that you can investigate. Camera patrols and audits may catch this behavior.

Another popular employee scam is over-charging on the bill. If the server acts as the cashier, then it is a simple case of adding an amount to the bill or entering a higher amount on the authorization and pocketing the difference. If the waiter is not the cashier, he may just add extra items to the bill to raise the total and increase the gratuity. This is more likely in large groups where the payer is not likely to verify the charges on the bill.

A final scam for you to look at is the food cashier who works in a snack bar or deli-type food outlet. Guests often use credit cards in these establishments but are likely not to leave a tip. The guest presents his card, the cashier prints the ticket for the amount, and the customer signs it, leaving the tip line blank. After the guest leaves, the cashier adds a couple of bucks to the tip line and re-authorizes the amount in the register. The cashier pockets the tip amount. The guest is likely not to notice on his statement that he spent $14 instead of $12, so nobody finds out.

RECEIVING

Receiving has many points in the process where theft can occur. This area generally encompasses the dock, storage areas, and any place where goods are taken into the property. Receiving is where the Purchasing Department connects with the Food Department and other users of these purchased items. As we have discussed throughout this book, theft is most likely to occur when cash and merchandise change hands. Because this is the main function of this department, controls need to be created, followed, and enforced strictly to protect the assets.

The basic process of receiving goes like this. A department, such as Food, places an internal order for more items. Purchasing places the order with the outside vendor. These orders are sent to the dock where they are used to verify that we received everything we ordered and everything that was delivered was ordered. Those verified deliveries are placed into internal storage where they are again ordered by the department on an as-needed basis. You can see where controls at every step of the process prevent theft if the controls are audited.

Outgoing Theft

One of the most common forms of internal theft does not involve receiving at all. It is usually very easy for employees to obtain merchandise that is in their control, such as meat, liquor, or other valued items. The theft occurs when they try to get it out of the building. Trash is generally associated with the receiving dock because they are in the same part of the building. It is important to keep the trash area separate and its access supervised so that items from the building are not brought out, and received items are not transferred over to, the dumpster for later removal. Security should be present when trash is removed from the locked trash area.

Receiving Theft

Merchandise is most vulnerable after the receiver has verified that all items on a packing slip have arrived. Now the property is owned by the company and in the possession of the person moving and storing it. A trash diversion as described previously is common here. Simply grabbing a bottle of liquor and putting it in a locker, delivering a case of extra meat to your friend in the kitchen, or even consuming a six-pack while working can easily go undetected here. Security patrols and audits are good deterrence, but an additional control of having the internal store receive the items from the dock is better. The store's supervisor or audit control should be doing inventories to make sure that what we think we have is what we have. Do not wait until three cases of tequila come up missing from storage to learn how the process works in your hotel. Sit down with the Purchasing Manager or controller to understand the safeguards already in place and to make sure they are adequate.

False Orders and Return Thefts

A slightly more complicated theft is the false order. The receiving clerk says we are all out of steak so he has Purchasing place the order. When the steak arrives, he can do several things. One is he can receive it, sign the driver's paperwork, and throw it in the back of his truck. Two, he can receive it, signing that it arrived and was placed into inventory, and then take it. Three, after receiving it, he can fill out a return slip that it was bad and had to go back, and then steal it. All of these thefts can be caught in the audit process, but can sometimes take weeks to process. By that time, everyone has forgotten about the delivery and because they cannot find the stuff, they just chalk it up to a mistake. Dual controls or a second signature help prevent these problems.

Lost Merchandise

Not all losses in Receiving are intentional. Items are lost or misplaced regularly. Security may or may not get involved in investigating or even mitigating these losses until it reaches a certain dollar amount, and someone wants some answers. So, it behooves us to make sure controls are in place to protect against loss, and that those controls are strictly followed. You are correct in that Receiving management and Accounting are more responsible, but they may not see the vulnerabilities that you would see in an assessment of that area.

Do not wait until the big investigation to learn the process. Right now, there are deliveries being made without invoices or signatures, receivers signing without verifying, and shipments not being fully opened and verified. To make it worse, nobody is reporting these losses. They will probably write them off as unknown losses or as items consumed.

I hinted at some of these controls previously, and the department knows which work best, but you may have to help enforce them. This is part of the job of protecting assets.

HOUSEKEEPING

Guest-room attendants normally do not handle cash, so internal theft comes in the form of guest property or company property. Strict lost and found and key control policies are important here.

SECURITY

Yes, security officers steal also. Collusion is one common way because Security is often used as the verifier on transactions and they see how all the processes work. Security also has the ability to take from lost and found or make false returns on property. Another one that I have seen too often by officers is a “drunk roll.” An officer may accompany an intoxicated guest to his room and then take the guest’s money without him knowing.

There are many other internal theft opportunities. If it is possible, someone will find it. The best way to prevent it is with strong internal controls. Keep an eye on other properties. If someone thinks of a way to steal something at another hotel, he or she is bound to try it at yours—or maybe already has.

BACKGROUND CHECKS

So which departments should have background checks on their employees? This is a trick question. And the answer is, all of them. I have seen many hotels that decide the only employees at risk of stealing are Security, housekeepers, and maybe managers. Even if that were true, stealing is the least of our concerns. First, any employee can steal—kitchen workers, receivers, cleaning staff. Second, workplace violence, sexual harassment, drug sales and use, and even poor work performance can be larger risks and create more losses for the property than simple theft. Any employee can participate in these illicit activities, so it is not logical to pick and choose who will have their history investigated.

Many organizations task the Security Director with doing background checks for all employees. If you do this, you know how time-consuming it is. I strongly recommend finding a contract provider to do this for you. It is well worth the price to have an outside company do your background checks. Criminal history is important and you need to check each state in which the applicant lived. This is time consuming and may be costly. This will actually cost you less if you compare like services. The background company knows what and where to check, but make sure the service includes what you want. Consistency—a common theme throughout this book—is key to your fair hiring practices. Imagine trying to defend why you spent hours checking the background of a person of one race, then spent days on a person of another race.

Timing of background checks is just as important as the complexity. In the last century, when a background check required a lot of legwork, many organized crime rings knew how to take advantage. Groups of immigrants from Mexico and Asia, knowing that background checks from their native countries took longer or were almost impossible, would come into a hotel filling those difficult-to-hire housekeeping positions. In cities where hotels were being built at an incredible rate, such as Las Vegas, managers needed housekeepers in quantity, and they needed them immediately. They would hire them first and worry about the background check later. Housekeepers clean about 16 rooms a day and have access to others, so 10 housekeepers in one day could “clean up” 200 rooms and be out before the background check even started.

There are two morals to this story. One is that backgrounds should be completed before an employee starts working. Second is the hiring of immigrants. Legal immigrants go through a long process of obtaining a work visa or resident alien status so they can work legally in this country. Therefore, they should have some work history in the United States, even if it was under-the-table or as a student. If they have a Social Security number, it should be traced to determine if it was newly issued or whether someone else may have had it before. Once again, this is a complex issue and should be given to experienced professionals.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

9

Executive Skills

FINDING YOUR PLACE

This chapter is 100% subjective. It is my opinion, but that opinion is based on observing, working with, and interviewing Security Directors worldwide. I have taken the good traits from those I admire and those who are successful and outlined them here. (I have even used a couple of the less successful ones to prove my points.) Everyone has their own style and these suggestions may not be part of yours, but I ask that you take some advice from the experts. That advice is presented for you here.

As the director of Security for your property, you need to decide what role you want to play in your corporate organization. One observation I have made is that Security Directors fall into two general categories. First is the passive response agent who is called up to the executive offices whenever anything happens related to Security. This director is generally told how much money he can spend, what size staff he needs, where his cameras will be placed, and when he needs to do something different. This director prefers to fly low and avoid problems and just wants to appease everyone.

Second is the director who takes a leadership role in the executive team. He presents himself as not only the Security expert but becomes a spokesperson for the guests and what is best for them. He realizes that Security is everyone's concern and collaborates with all departments to make sure his needs are actually the needs of the entire organization. This director is seen as the expert on property, and nobody would think of making decisions without him.

As you might imagine, my preference is for the second director. He or she will be more productive, more effective, and will be better compensated and more successful in the long run. Ironically, this proactive approach goes right along with the preventative nature of our industry. These are my observations and solutions for attaining this level of leadership at your hotel.

You have three responsibilities as an executive in your company. One is to your boss and the executive team. Two is your responsibility to your staff and their development. Three is the responsibility you have to yourself and your personal growth. This chapter will devote itself to making your company, your department, and you as successful as possible.

DOI: 10.4324/9781003037644-9

I have noticed that the office of the Security Director is placed somewhere in the hotel away from the "C-suite." Marketing, Sales, and Operations are all there in the executive cluster, but Security is down in the basement. There is probably a practical reason for this, but it is also symbolic of the pecking order in a hotel. There are advantages and disadvantages to this separation, so make the best of the positives and reverse the negatives.

Cooperation and Collaboration

Let's talk about your place in the grand scheme of things. The perception everyone has of you and what you do is based entirely on you. Without a proactive approach to becoming a part of the team, the other department heads and even your boss may consider yours a supportive role. Worse yet, they will consider you and your department a necessary evil. This image probably comes from our predecessors who were perceived as gorillas, called in as the muscle to take out the trash. We need to put as much distance between us and that horrible, negative image as we can.

Allen Pinkerton was born in Scotland and became a successful businessman in the mid-1800s. His unwavering ethics and appreciation for protecting business from those who would harm it soon earned him a reputation as the first private detective. Spying against the Confederate Army and protecting industry from some of the dirtier union organizers built his reputation into a formidable business of its own—the Pinkerton Agency. In 1871 when the Department of Justice was formed, it did not have the budget to train and staff full-time investigators, so it contracted with Pinkerton. This relationship lasted about 20 years and was terminated by federal law. So you might say that the country's first organized police agency was really a security company. Many of us in industrial security still trace our beliefs and our philosophies back to Mr. Pinkerton. Pinkerton's legacy lives on as a division of the worldwide Securitas Company.

Start with your place in the organization. If your current situation allows a department head to tell you to install cameras in a certain location or provide security for a particular event, you are not being a director. You need to get yourself into a position where you collaborate with your colleagues and come up with solutions together rather than being told how to run your department. You have to bring yourself up to an equal playing field. This is not a competition; it is about a well-rounded team where each member has his or her expertise. Your expertise is security.

Expertise is the key. Building your expertise is discussed in the personal growth section of this chapter. In this section, we detail how to offer it to the team. Start by playing offense instead of defense. Get out in front of situations instead of waiting for the call that tells you what to do.

If you can get up to that level where you are an equal—one of the executives who has an equal seat at the round table—take it a step farther. With security in your blood, you have an advantage that you need to impart to your colleagues. You are used to operating within a team, where everyone operates toward the same goal—the company. Your fellow executives—Sales, Marketing, Operations—have made their way in the business by competing with each other. They probably think and act more vertically (some call this "kissing up") than they do horizontally (as a team). Your security DNA is of a different type. You realize as a team player that competition with your colleagues, even if it is only for attention from the boss, is counterproductive.

As you excel at the collaborative model, you will be known as a team player, one who is comfortable with his or her place and does not feel a need to compete for attention. I guarantee your boss will notice and will start using you to team-build and problem-solve. Are you still fuzzy on this concept? See if this example hits home: There are a couple of department heads that are so busy worried about what the other is doing, who will get their idea to the boss first, who gets a bigger piece of the budget, and who will blink first, that they are not getting anything done. You explain to your boss that you have already put together a team of select department heads to solve a certain problem. Your boss will notice this behavior and will reward you with more responsibility. When he or she has a new initiative or sets up a new working group, you will be likely the first choice. Your boss wants global thinkers and not those who operate in their own silos.

Executive Meetings

Chances are, you are involved in some regular staff or operations meeting. If not, you should be. Study the agendas of these meetings and come prepared. Take note of plans to host special events, celebrities, and public officials. Use the contacts you made in your networking (see next) and investigate places where they have stayed before. Someone else has already managed this security issue, so take advantage of his or her experience. Your value increases when you come to a meeting prepared to discuss security concerns that Marketing has not considered.

Once you become a member of these collaborative sessions, make your input positive. The reason you were probably not considered initially is the perception that you will be an obstacle. Frankly, we in Security do tend to make ourselves obstacles by saying, “It will not work,” “I don’t have the staff,” or “It will cost too much money.” Look, think, and present yourself as a company person. Offer your objections only if you have a solution (e.g., we may have to spend a little overtime, but it may be worth it to get our name out there. Or, that group tends to cause trouble at conventions, but that is why you have such an effective Security Department). Instead of saying no, you are saying yes and are providing valuable input.

Set up individual meetings with the departments you work with most. Risk Management, Human Resources, and Facilities, for example, are probably the departments you support. Work out problems before they occur. As mentioned previously, do not be an obstacle. Be willing to do anything you can to make their job easier and they will return the courtesy. Once you get comfortable with this process, try it with departments with which you may not work as closely. Go over upcoming events with the catering manager. Let him or her know you will not be an obstacle, but a resource to make the events run smoother.

You don’t like hearing on Friday that there is going to be a group of 500 fraternity students staying in your hotel on Saturday. The Sales Department does not tell you because either they don’t consider your opinion important, or they fear you will throw up barriers. Work with these event planners so that they will tell you far in advance so you can make your own plans. Explain your point of view and that if you have time to prepare, you will not be an obstacle, but a willing participant. Either the fraternity group can trash the hotel, or they can provide a lot of revenue, depending on how much time you have to prepare for them. As you offer your expertise, such as segregating the group from other guests, adding officers here and there, closing the pool, and so on, you will become known to those event planners as a resource.

Nothing is more frustrating than having the rest of the team plan a remodel or new addition without consulting Security. As they design and build a new bar, for example, they get caught up in the architecture, hiring, marketing, and menus and take for granted the placement of cameras, access control, type of clientele, etc. Approach this as with the meetings discussed previously. Get in on the initial planning and become a resource instead of an obstacle. Instead of whining that a bar will bring fights and problems and ruin our business, explain how some basic, cost-effective controls can reduce many problems. Show how properly placed controls will prevent theft and reduce loss.

COMMUNICATION

> Don't do anything I would do, and definitely don't do anything I wouldn't do. There's a little grey area there, and that's where you operate.
>
> *Iron Man* Movie

Communication is a big word in business, emergency response, report writing, and many other topics covered in this book. Executive skills are no different. A leader who cannot communicate up, across, and down the chain of command is going to struggle, especially if he/she is a new leader.

As we have learned throughout this book and I am sure in your own experience, communication is not only about the written and spoken word, but includes body language, listening skills, behavioral assessments, and even timing. I will not be covering all of those things, but instead I offer some tips that they may not tell you at school or at a meeting. These are the nuances I believe are important and of course there are different styles with different smiles, so view this one through your lens and see what you can pick up.

The Boss

Set up regular meetings with your boss. This is a chance to let him or her know what is going on in Security. Concentrate on what Security brings to the bottom line—losses recovered, losses prevented, and situations resolved. Do not wait for this meeting to notify the boss of important incidents. You never want him to hear from someone else what he should have heard from you. Establish in advance the types of notifications to provide (fires, fights, internal thefts), by what means they will be given (phone, email, in person), and when (immediately or the next day). I have seen how department heads will race to the boss to reveal some juicy information just to receive favor for being first to report. Do not let this bother you, as you will be following a protocol that your boss prefers.

Without dipping too much into your own personal style, I want to stress the importance of your relationship with your boss. We Security Directors tend to be quiet but honest, reserved but capable. Unfortunately, it does not matter how good you are if the boss does not know it. You may need to manage your boss a little so that she knows you exist, trusts your judgment, and has you in mind when raises, bonuses, and promotions come along.

Start by keeping regular meetings with your boss. Have a weekly regular time set up (every Friday at 2 p.m.) and have some ammunition ready for those impromptu meetings. Come to the weekly meeting with your own agenda or notes on what to discuss. Bring a brief summary of your payroll, expenses, or financial status. (She already knows but wants to know if you know.) Lay out briefly what you are doing to reduce expenses or overtime (before she asks). Summarize any big investigations, major incidents, or ongoing problems that your department has solved. Do not sugarcoat. The boss wants to hear your challenges as well as your successes. If you do not have the answer, ask for advice. Most executives want to hear that you will seek help when needed. Perhaps it is a problem manager or a rash of vehicle burglaries.

In addition to the weekly meetings, always have something ready for the "elevator meeting." You may run into your boss in an elevator, the parking lot, or the lunchroom and you need to be prepared to speak of something besides the weather. We caught the guy stealing towels off the maid carts, or I think I found a better source for DVRs—I will have a report for you Friday. Better yet, be ready to answer his questions about overtime, who parked in his parking spot, or what the occupancy is.

Keep track of your personal and department task list. If you were given an assignment, or you mentioned at a previous meeting that you would see to some project, keep a mental list of that progress. Have this information ready and keep the boss updated. I completed the background check you asked for, compiled the stats of how many towels were missing year-to-date, and got prices on the new uniforms. I have not yet completed the yearly loss report, but I will have it Monday. Your secretary has the other reports. Keep your accomplishments on the top of her mind so that when the big assignment or even promotion comes up, the recollection of your performance is positive. Remind yourself that in Security, your achievements are not always obvious, and you need to blow your own horn.

I mentioned in the beginning of this section that you want to avoid getting too comfortable. This is not where you want to be because others will resent you and your time will be short. Nobody likes to see someone kicking back, skating through the day, while they are working their tail off. If you find yourself with nothing to do, or that you are spending more time at work socializing and butting into everyone else's job, you are too comfortable. I am not telling you to fake being busy because you cannot sustain that. You need to challenge yourself constantly. First, you are fooling yourself if you think your property runs perfectly and is crime-free. There is always a project you can initiate to further reduce crime or increase guest satisfaction (see Chapter 11 for some hints). Self-motivators are successful executives. Keep running, keep challenging yourself, and keep making your job better.

Your Staff

Other departments actually expect Security to be the experts at communication. We developed the pre-shift briefings, we use radios, and we document the important stuff in our reports. Make sure you practice this good communication both ways between you and your staff. Let them know what is going on with the property as soon as you can, before they get the information elsewhere. Security officers like knowing things first—everyone does. Take notes at the meetings that you attend and create a process so you can get that information to your troops immediately.

Create a process where you know everything your staff knows as soon as it happens—24/7. Whether it is phone calls at all hours, text messages to your company phone, or emails to your iPhone, you should be available at all times. Do not feel bothered when you are called late at night. You are happy to hear it in real time rather than from your boss in the morning.

Many say that the success of a good leader is dependent on those with whom she surrounds herself. Your managers and supervisors need to have the same work ethic and be as smart as you. Some leaders are tempted to promote those who are good, but not good enough to pose a threat to their own job. When you think about it, that threat only exists in your own motivation. If you are following some of the traits and habits in this chapter, you will stay ahead and set the example for your subordinates. If they are biting at your heels to get your job, that is the best thing that can happen. You will have a stronger team and you will have some encouragement to stay current and energetic. Usually, the lazy manager fears his subordinates. He deserves what he gets.

Remember the secondary duty you have in any position in the company is to prepare your successor. This is often called grooming and is a requirement more than a luxury. How are you protecting the assets of the company if something happens to you and the department is left with no clear leadership?

First, you need to select one or more likely candidates. Do this by asking them what their aspirations are. If they are comfortable and just want to finish out a few years before retiring, or have their sights set on another career, they are probably not your best choice. However, do not forget that many of our best Security professionals were on their way to another career when they came across this one. After all, how many kids in the fifth-grade dream of becoming a Security Director?

Second, engage in some casual training. This type of training includes discussing certain factors in the decision-making process. Explain how you make decisions, prepare the budget, communicate with the boss, and handle difficult decisions.

Maintaining Morale

Transmitting news back and forth is one thing, but maintaining constant, open dialog is more complicated and, for some, more difficult to achieve. Many managers claim to have an open-door policy but keeping everyone satisfied takes a bit more than that.

Security officers may be some of the most difficult employees to motivate. Many, by their own admission, are either finishing out their careers, waiting for a better opportunity, or just plain lazy.

In my experience, Security officers are motivated in several ways. First, just as they said in their interview, they want to help others. Most of us feel a sense of satisfaction and accomplishment when we help someone through a difficult situation and use our unique resources to resolve it. Second, they may not have admitted to this one, but most want some action. That 1% of the time we get our adrenaline pumping is often the most satisfying part of our job. Third, and I really doubt anyone will admit to this one, is respect. As Security officers, in a position of authority, we like to be looked up to, give orders, and walk around looking handsome and professional.

Ask management if these motivators fit into their profile of the perfect Security officer, and they will definitely like number one (helping others), but probably are not too keen on numbers two and three: providing action and bossing others around. Most business operators want a Security force that is helpful, loyal, honest, and efficient. Imagine if you could combine the expectations of employees and management so that everyone is happy. Actually, you *can* give the officer those three things he wants (and more) and achieve a highly successful Security Department (and more). That is our job as Security professionals—to provide for the employee *and* the executives and operate a highly effective department—and here is how it is done.

YOUR PEERS

Networking

Networking is simply communication with various groups or individuals. It applies to all of these responsibilities you have to those around you, but I cover it here because it is often the most difficult because you have to meet and talk to new people.

Many of us security types are not comfortable with this process. We are somewhat private individuals who do not sell ourselves well. If you ever watch a salesperson network, it is almost sickening to people like us. We conjure descriptive words like "ass-kissers" and fakes. Believe me, I was the same way, and I am still somewhat uncomfortable with "small talk." Some Security Directors keep to themselves, talk to no one, and mind their own business. I do not consider them successful. Recall that example from the beginning of this chapter about the director who is more of a sheep dog.

One day, I realized that I did not need to sell myself as these salesmen do, but I did need to sell my hotel and my department to get what I wanted. Perhaps I felt like less of an idiot knowing that it was part of my job and not for my own career building. After that, I found it easy to network, make small talk, sit and converse with strangers, and build my address book. So, let's go through the networking process methodically because methods are our nature.

First, we need an objective. Why network? Your reason for networking is to share information. Unlike that camera salesperson who asks you how you are doing at every association luncheon, you are not selling widgets. You are selling anything you have to offer in exchange for anything you need from the other guys. Here are some examples.

When metal thieves steal your brass sprinkler fixtures, chances are you will file a police report. It goes to detectives, and it may or may not get assigned to a human, who may or may not go looking at the scrap yards for your brass. However, if you call that sergeant from property crimes who you met at the security chiefs' meeting last month, he will likely put some emphasis on your report. By the way, he also needs a favor. He needs to get a photo of a known car burglar out to as many security departments as possible. Suppose you send his email to all of your colleagues in the entire city and save him some legwork. There is nothing illegal, unethical, or immoral about this transaction of information, but it could not be done without a little networking.

Now suppose you are planning an exercise to test your new evacuation plan and you want the fire department involved. Call the chief who you met at a city council meeting last week. If they bring their engine to the hotel and spend a couple hours helping you evacuate your employees, you can let them use your penthouse floor to do some high-rise drills next month when the hotel is under construction.

Call or email your fellow hotel security directors and invite them to send a few officers to the CPR training that you are hosting next week. They will reciprocate when they have training classes of their own. If they cannot host some training, maybe they have some other amenities they can offer for the good of the group.

Information is our objective and we have some tools we can use to trade and to open up conversations. It is now time to start. I have found the best way to network is to get involved in as many organizations and groups as you can.

Government Meetings

City councils, committees, county commissioners, and any other governmental group is the best place to find police and fire chiefs, inspectors, code enforcement, city attorneys, etc. These people are much friendlier when they have met you and they know you are one of the good guys.

Associations

ASIS has a local chapter in almost every city and is a great way to meet like-minded people in your business. I always find it amazing that security professionals in other industries (retail, contract, utilities, manufacturing) have many of the same problems and solutions that we have. Other associations may have chapters in your town.

Local Trade Groups

I have mentioned Security Directors’ Associations, but there may be other security groups focused on retail, fraud, or other crimes. These are a must-join because this will be your base of contacts and where you give and receive all of your information.

Nonprofit Groups

There are always some community groups in every town that fight drug abuse, domestic violence, crimes against kids, etc. There may be a crime-stoppers or other citizen tip group that meets and exchanges information.

Public/Private Groups

In the past 10 years or so, local and federal government has really reached out to the private sector to battle issues of joint interest. Two that come to mind are emergency preparedness and counterterrorism. Every city or county is required by the federal government to have an Emergency Manager. Meet this person and find out what he or she does. They are usually very excited to get cooperation from private entities, especially hotels that can provide resources in an emergency. There are also fusion centers in every state that deal with terrorism among other things. They may have an advisory board or a communication group and they want to exchange information with the private sector.

Online

Finally, there are many groups on the Internet that network and share information. Engage these to your comfort level, but I find that I learn more from these people than anywhere else. The best way to get your feet wet is to log on and observe the conversations until you feel comfortable.

Regional Training

I mentioned several groups and agencies where regional training is a benefit and is probably already being planned. Airports, school districts, and fire departments do all kinds of regional training. Start by observing these exercises and using those network skills. Find out what your hotel's role would be in a disaster and which one of these agencies would respond to your facility. You can learn some valuable emergency training skills from these people and maybe offer some resources in return.

Regional Communication

Two of the groups I mentioned previously are keys to your regional communication trees. Your local Security Directors Association and Fusion Center are all about communication. The Directors group should have a listserv of email addresses that can broadcast information instantly. This is invaluable and necessary in every community. If you do not have a group like this, start one or join one in the next town. The Fusion Center will usually proclaim itself as the focal point for dissemination of official government information of importance to the private sector. Make sure you are on its mailing list.

Mutual Aid

The concept of mutual aid is generally considered a government relationship. Fire departments have aid agreements to assist each other when their resources are overwhelmed. Police departments call the next county when they need specialized training or equipment for a hostage situation. Private enterprise has actually been using mutual aid for years. You might be surprised to find that your own hotel probably has agreements with other hotels to "walk" guests in the event of an over-booked situation or a catastrophe.

In September of 2017, Hurricane Irma ripped through the Caribbean and Florida, causing widespread damage. A senior care facility lost 14 of its elderly patients when they lost power and air conditioning. Most believed to have died from heat-related illnesses.

The care facility was sued for wrongful death and negligence for not having or exercising appropriate backup plans for loss of power. No calls were made to 911, the hospital across the street which had power was not utilized, and records of the deceased were allegedly altered by the health care workers.

These agreements between companies tend to be verbal, which have no teeth. In the event of an emergency, what will be your recourse if that other hotel decides it does not want to participate in the agreement? What if the other hotel does not even know what its responsibilities are to your organization? This agreement that was based on a handshake might cost millions of dollars if someone breaks it. Your insurance company and lawyers are going to be looking for someone to blame. You don't want to be the one who made the handshake with no documentation. Therefore, you need a written agreement.

Written Agreement

This is a step-by-step process to create a Memorandum of Understanding (MOU) for mutual aid. Start by determining your needs. What is the agreement about? (Evacuation space, food for displaced guests, hotel rooms, etc.) Then meet with the key personnel of each property that makes those decisions. When a verbal agreement has been made, document it as "the purpose." Next, on the document state the authority by which it is made. (This is normally for governmental entities, but we can state that it is between management of each property.) Then we specifically list control and coordination of the agreement. This means who will be in control and who will coordinate these mutual activities. In other words, who is responsible for adhering to the agreement? Then specifically list the responsibilities of each department and each person if necessary.

The next part of this document covers the post-incident information. Compensation is an important one. Who will pay how much for what and to whom? How is insurance involved in that compensation? Who assumes liability for certain activities on which property? Finally, the document is signed by authorized representatives from each property.

This sounds complicated and is too much information for a couple of paragraphs. That is because you will not write an MOU based on this book. Your legal folks have boilerplate agreements ready to go and you can probably fill in the blanks at their advice. If you are not using a lawyer, there are plenty of sample forms on the Internet.

Sharing of Resources

I always thought it was ridiculous that two hotels sitting right next door to each other have two separate shuttle buses, separate lawn mowers and snow blowers, and even 50-foot freeway signs. These have nothing to do with Security, but wouldn't it be nice if we could share some resources to save money? Those same two hotels might have perimeter cameras that look at the same area. Why not share cameras and pipe the feed into each hotel?

Consider people resources: The two security officers from each property probably pass each other doing their perimeter checks. What if Hotel A did it on the hour and Hotel B did it on the half hour? This reminds me of those old World War II movies where the German guards are on one side of the border with a gate and the Russians are on the opposite side (a foot away) with the same setup. Okay, they were enemies! Our two hotels are not enemies—they should be allies working toward the common goal of protecting everyone's assets.

The same applies for training—and this is where you can save some real money. It makes no sense to have one hotel train three officers for 40 hours and have another hotel do the same thing the following week. If you combine these resources, you not only save the money of training, but also you make your security programs more consistent. You read in Chapter 1 that your security will be compared to other properties in the event you are sued. What better defense than having the same training as your neighbors.

Regional Disaster Planning

In Chapter 7, we talked about emergency planning. Above, I mentioned the close relationship you should have with your regional emergency manager. This is where that comes together. When I first assumed my position, I started asking around about emergency planning. You have a fire, a broken water main, a gas leak—no problem. You evacuate, call the authorities, and they take care of the rest. Not exactly. They need you and you need them. Get involved in their meetings, their exercises, and offer up some assistance in advance.

Besides the horrific images of death and destruction coming from the ruins of the earthquake in Japan in March 2011, we saw business continuity break down as well. Those who had mutual aid agreements, contingency plans, and backups of backups never imagined a disaster of that magnitude followed by a tsunami of even greater devastation. One example was airports. Imagine the hundreds of flights on approach to one of the island nation's many international airports. As one Delta pilot reported, they were on their final approach with little fuel, and their airport was under water. The backup airport was also devastated. The backup to that airport was already filling fast with diverted flights. The pilots had to do some fast thinking to find landing places before their fuel ran out.

Consider your plans in the event of a regional disaster. If you have agreements with other hotels, what will you do if they are also out of commission? You may not be flying an airplane, but you are responsible for hundreds of people that need a place to eat and sleep.

In 2011, a contestant plane at the Reno Air Races crashed into the stands causing a mass casualty incident and a regional emergency response. Because we had already promised our services, the hotel was the official hotel of the incident, housing doctors, coroners, and others who had been flown in to assist.

The moral of this story is that you need to talk with these people before a crisis hits and not during. Since we set up the initial agreement, that community has been one of FEMA's models for Public/Private partnerships in the US.

PERSONAL GROWTH

The final responsibility I mentioned was to yourself. Start with education and experience. If you are lacking in experience, you must network and learn from others. If you lack education, it is not too late. Most employers are happy to support continuing education if it benefits them. Obtaining a certification like Certified Protection Professional from ASIS is a great example – but there are others – to advance your education in security. There are also certifications and classes provided through your local university, FEMA (the Federal Emergency Management Agency) and DHS (the Department of Homeland Security), and many other organizations. Do these on your own time if you need to. Classes not only make you more knowledgeable, but also you will find that they motivate you to think of and try new things. They also are a great networking experience, which I will discuss more in length later.

Once you get your personal growth on the right track, you need to start attending meetings and conferences relative to your industry and to your market. This will do several things for you. You will network with other professionals in similar situations. They will learn from you and you from them. These will become your resources when you need advice for a challenge that is new to you. You will find that whatever it is, someone else has already experienced it and can help you through it. Conversely, your peers may come across something in which you have experience and you can return the favor.

Your Work Ethic

Another thing I have noticed with Security Directors is that they are usually overwhelmed or lazy. Maybe lazy is too harsh of a word, so let's call it "comfortable." You can probably see yourself in one of these two categories and I hope you see the disadvantages of each.

The overwhelmed director runs on a high level of stress because he does not delegate enough, has inadequate staff surrounding him, or takes on more than he can manage. The comfortable director tends to have plenty of time for golf, takes weekends off, spends time talking with colleagues (nothing to do with work), and appears a little too confident. Ideally, you find your place somewhere in the middle of these two stereotypes. Look at the following suggestions for finding that middle ground.

Stress

The more responsibilities you have, the higher your stress level. It is not all about work; we all have bills, car troubles, family problems, and other stresses at home. Add to those layoffs, downsizing, bad economy, revenue drops, and grumpy bosses. Don't forget that you manage a staff with all the same problems you have. The way we handle or reduce our stress not only affects our own family and work, but also it sets the tone for our employees to deal with their own issues. If, for example, you yell at others to cope with your stress, that behavior snowballs downhill until the entire department handles all conflict this way.

This entire book is devoted to making your job easier, which is definitely a stress reducer, but here we will talk about ways to avoid and diminish that stress if it does pop up. Before we begin, acknowledge that stress, and even anger, are natural emotions. Do not feel bad, or less of a manager, if you feel them.

I am not a doctor, so I will not pretend to advise you on your physical or emotional health. Take these on with a psychoanalyst, physical therapist, or dietician. What I can do here is help you keep those causes of work stress down. It is true that rest, proper diet, and exercise are huge factors in reducing stress.

Time Management

When we run out of time, we have to neglect (or we forget) something we have to do. Keep a schedule, such as Outlook, so you do not double-book or overlook important meetings or events. Put everything in your calendar or you may forget even routine things like "walking around talking to employees" or "read incident reports." This will hold those places to keep you from blowing them off to go to a meeting. If a meeting is scheduled during your email reading time, reschedule the emails. When you get to the point where you have so many meetings that office or floor time is impossible, something has to go. Delegation is a positive way of duplicating yourself.

The stress is not generally caused by one event, but usually not having the time or resources to deal with that event will contribute to it.

Delegation

If you go to so many meetings that it exceeds your work time, you have too many meetings. Decide which ones can be delegated to a manager or administrative assistant. Delegation not only duplicates you, but it empowers and trains those who answer to you, to learn your job and how to run your department. If you spend a lot of time on interviewing job applicants, maybe you need a hiring manager. If you attend many meetings to coordinate special events, perhaps you need a special events manager.

When delegating, make sure you take the time to train that subordinate on the subject matter, the limits of his authority, and the background he needs to properly address the situation. Make sure he reports to you, but also make sure the report of the meeting is not as long as the meeting itself. That saves you no time at all.

Visibility

The Security Director should be the most visible person on the property. It is your responsibility to know every employee on every shift, especially your own staff. Set a time each day to get out and meet the employees and the guests. Set time each week where you work a different shift. Seeing the boss is a real morale booster and makes you part of the team, rather than a memo writer in an office.

Besides being visible to everyone, your demeanor at all times should be above reproach. Visiting the bar after work, flirting with employees during work, and driving erratically through the parking lot all look bad and set a poor example. Remember that everything you do will be watched and scrutinized more than anyone else. This is partially because you are an executive and partially because you are Security. Employees will look for a double standard and assume one exists even if it does not.

Punctuality is a trait of a good leader. If you tend to be late, it shows that you do not manage time well. Awake earlier, leave for meetings earlier, and account for problems on the way. Do what you need to do to get to work on time and keep appointments.

Respect

One of the hardest personal traits for managers to achieve is respect. Many mistakenly place the desire to be loved over the need for respect. When decisions are made because a manager wants to be nice instead of what is best for the department, personal ego is now running the department. Some decisions will be difficult personally, but if they are in the best interest of the company and everyone understands the mission is to protect the assets, then the decision becomes clear to everyone.

When everyone is treated fairly and equally, respect will be almost automatic. Not everyone will like every decision, but if it is made for a good business reason, they will respect and understand it. My advice here is treating everyone you encounter, employee or not, as you would treat your mother, your boss, or someone whom you respect. You will feel better about yourself and those around you will respect you for it.

Attitude

Attitude is a big part of being overwhelmed. We have all seen how the exact same event affects people in different ways. Everyone looks upon your behavior, so you need to be the model. Panic is a big stressor for people who feel overwhelmed. Being in Security, you probably have this under control. Perfectionism is another personal habit that leads to stress. If you expect perfection from everyone and everything, you are going to be disappointed often. You will never be satisfied, always stressed, and never get anything done if you expect perfection. I have seen this consume ineffective managers. That is not to say that you should not expect tasks and assignments to be completed correctly. Just cut down on being so "nit picky."

Negativity is an attitude that seems to permeate an entire organization when just one or a few people practice it. People choose to be negative. As mentioned previously, the same situation can be accurately perceived as a positive by one and a negative by another. Just prior to writing this paragraph, I told two people that I was having new shelves installed to store office supplies. The first person was very excited that her job would be easier and it would take less time to find supplies. The second person commented that it would probably take a week for our engineers to install and paint the shelves. Then he complained about having to learn where everything was. Two people. Same event. One positive and one negative. Think about the attitude that you model for your employees.

Breaks are important enough that we make our employees take them. They reduce fatigue and allow the mind to clear. Make sure you take breaks as well. Avoid lunch at your desk and take time to walk away from a problem, if you can, to relax and clear your mind. Overwhelming stresses can seem much less significant the next day. Besides, break time is a great time to interact with your employees.

Another method to deal with stress is to talk things out with peers. Avoid sharing problems with subordinates. Perhaps another department head or someone away from work can provide advice, but also be a sounding board as you vent. Be sure not to vent to those on your team. This is explained in another section.

Your personal demeanor is important to everyone. Being seen intoxicated, even off-duty, or in your grubby clothes can tarnish your image. How do you expect your boss to be dressed? What would you think of her if she were not dressed to your expectations? What do you think your employees expect? Decide on an image you want and stay with it. Imagine a major incident occurs at your property late at night and you decide to head down there and take charge. Maybe the media shows up and you need to make a statement. Decide on the image you want for you and your property and present yourself in that way.

Tactical Planning

This strategy has been mentioned several times throughout this book and I cannot stress enough how this can change your style and improve your efficiency. Whenever you make a decision or plan anything, start with your objective. Once that is decided, work backward, meaning: figure out what needs to be done to reach the objective. Here are some examples.

1. A fire truck is in route to a house fire. Smoke can be seen from a distance and upon arrival, the house is fully involved. It is 3 a.m. so presumably people are inside. The team with one truck could probably extinguish the fire pretty easily if that was their objective, or they might just let it burn, if possible so as not to get anyone injured. But that is not their objective. Their objective is search and rescue of possible occupants, so resources will be used to protect firefighters going in. The firefighting strategy changes drastically.
2. (True Story) Boss calls several of us to a meeting about a specific item involving our relationship with city officials. He talks for about 30 minutes about nothing in particular, then finally says to me, you are better at this than I am, why don't you lead the meeting.
3. Think about the navigation app you use for driving. It starts with the destination and works back before it even tells you to start. If it tried to guide you as you went, it would likely take you on a few wrong turns.
4. Finally, compare your active shooter response with that of the responding police. I have written both, and I can assure you the objectives are entirely different. The objective of the police is to stop the assailant. Their plans include immediate confrontation, coordinating officers, and a constricting perimeter to stop the assailant. Your objective is to evacuate, attend to injured, and direct police.

I urge you to give this a try for everything from eating at a buffet to conducting a focus group.

BUDGETING

The budget is really the biggest difference in Security policy from one property to another. We all want to protect our guests and we all want the best equipment and highest paid staff, so the only thing that usually separates us is the amount we spend. In this chapter, we will talk about how to prepare a budget and then look at some creative ways to save and get more money to do the job you would like to do.

Basics

You did not sign on for all this paperwork. My gosh, the numbers, spreadsheets, math, one-track controllers. When you run a department, you have an obligation to manage your money. I will try to make this simple, but reach out to someone if you need help. When I took over my security department, another department head was doing my budget. I was shocked! She said the last guy could not figure it out. No wonder we never got any new equipment or raises for our troops. I was mortified. I went to the boss and said, let me do it. He agreed. You can do it also. Let's go.

What Is It?

My apologies if this is too basic, but I want everyone on the same page. A budget is the framework for your spending. At home, if you know you will earn $1,000 (revenue), you divide it by groceries, mortgage, utilities, your Amazon habit, and the rest goes to savings. That is a budget. Oh, if it were so easy…

That is basically what we are going to do. Security is a "Non-revenue-generating department." This means we do not bring in any money for the company. That saves half of our time already. We will be given a certain amount to spend—usually the same as the prior year—and we either budget to break even, or we add and subtract depending on what the boss says. Cut your expenses by 10%, or we should have more events next year, or everyone gets a raise in June so figure that into your budget. So let's start with our base number (allocation, spending limit, budgetary limit).

Prior Year

Prior Year (sometimes called current year on your spread sheet) refers to the fiscal year that is just before the fiscal year for which you are budgeting. (A fiscal year is the 12 months used by the company for its budget—could be Jan 1, July 1, or whatever the company decided.) If your fiscal year begins May 1, you may be planning your budget around February. That means February, March, and April have not yet occurred, so you have no expenses to compare for those months. For those months, you would have to estimate how they are going to turn out based on how the other nine months did that year.

Process

You will likely be given a spreadsheet (Excel or something easier) with lots of numbers already filled in. It will have line items representing the categories of money you have spent and plan to spend (labor, benefits, maintenance, equipment, office supplies, uniforms, etc.). Columns representing the months will be labeled at the top. The basic idea is you look at what you spent last year in February and decide if it will be the same, more, or less. If your department is cruising right along, you can figure it will be about the same.

If you are looking at the 12 months for office supplies, for example, and one month is much higher than the rest, it is likely that a large order was placed last year in that month. Assuming you will use just as many paper clips as the prior year, then average out the 12 months so they are all about the same. If you do another large order, your accountants understand you will be over for that month, but that it will balance by end of year.

Full-Time Equivalent

Full-Time Equivalent (FTE) is a common and useful term in budgeting your staff. It is simply the number of employee positions you have, based on the hours worked. You may have 60 part-time employees who work a number of hours to equal 40 FTEs. This number is the total hours worked in a month divided by the number of work hours in the month (approximately 168). Since some departments have part-time employees and give extra days off, sick days, early-outs, and other variables, FTE allows you to compare wages evenly from year to year. FTEs are generally another line item on your budget. If you brought in extra troops in August for a convention, your FTEs will be higher, even if you did not hire or fire anyone. FTE counts hours, not bodies.

I guarantee this line is where you will be scrutinized. Why is February forecasted to be 12 FTEs and you used 10 last year? Or why did you use 12 FTEs in February when in prior years it was 10? This budget requires a bit more calculation than your office supplies. You may or, depending on the detail expected by your controller, must drill down each month, each day, by shift to determine your labor. Sometimes it is easier and acceptable to just copy last year’s numbers.

Wages

Wages, the largest part of most security budgets, is usually divided into hourly, salary, and overtime expenses. These amounts change year to year if your staffing numbers change or if your hourly wage changes. If you provide a cost-of-living increase of 3% each year, then you would add 3% to the hourly and salary amounts. If you downsize your department by six positions, you would subtract those six salaries from the budget.

Recurring Expenses

As the name implies, certain expenses occur every month and they are often the same. They may be your portion of company-wide expenses such as phone or laundry. This just simplifies your data input as these rarely change.

Overtime

Overtime is usually not planned in a budget. The objective is to operate without overtime, so it is usually calculated into the hourly amount. In other words, use the sum of the prior year's hourly and overtime amounts to equal the hourly amount in the new year. Overtime would be forecast to be zero. Wages might be separated further into holiday, vacation, bonus, commission, and other amounts included on employee checks. They are budgeted in the same way.

Benefits

Benefits are a cost we often neglect. Your accounting department does not. These carry over to the next year consistently unless there is a significant change in benefit costs. You likely will not have to worry about that. Benefits include cost of health insurance, life insurance, retirement, etc.

Budget Submission

The program given to you to input your numbers is easier than it looks. You cannot break it. They will not give you the master budget for you to add zeros and decimals. In fact, you can play with your numbers to see what your bottom line would look like if…

You will likely have to justify changes in line items from prior year (up or down). This could be a field on your spreadsheet or it's a separate document. Take this to the controller and ask if you are correct.

> In 2005, security officers at a large hotel in Nevada filed a class action lawsuit for back pay. Officers asserted that they had been forced to come to work 15 minutes before shift for a briefing without compensation. They also said they were routinely called off of their lunch to respond to calls, also without being reimbursed for missed break time. The hotel maintained that the 15-minute briefing was compensated by adding time to the lunch break, and that the missed lunch breaks were either paid overtime or made up later in the shift.
>
> The hotel finally settled with the officers, paying them back pay for the briefings and establishing policies about unpaid time.
>
> After many other lawsuits and complaints to Labor Boards, corporations of all types have determined that it is easier to be fair and transparent in paying employees for briefings, mandatory meetings, and training.

Your Budget

You are responsible for this budget, so take ownership of it and follow it. Doing these calculations and forecasts will help you stay on track. You will see where your department is spending money and possibly even find ways to save money. When the boss tells you to cut your budget by 5%, you will have an idea where to start looking and what impact it will have.

Look at your budget as the general manager will. He is supportive of security's efforts and he knows it is necessary, but he would still like to have the money he spent on security to spend on painting the building or buying some TV commercials or whatever. She will also be looking for places to save. Beat her to it and show her what a talented department head you are.

Capital Expenses

Return on Investment—What is it and how do I get some?

Capital Expenses are requested annually (usually) but may be distributed quarterly or annually. At a certain time of the year, each department will be asked for their shopping list. This is where ROI comes into play, because Capital is like a loan from the company and ROI is how the loan will be repaid. Since Security does not make money in most companies, the return has to be explained or justified differently.

Because of tax laws and sustainability, your company will likely not let you use capital for the following: Additional Staff; classroom training; overtime; travel to a conference or the conference registration; items below a certain dollar amount—these are expenses and go in your operating budget.

Life Safety

Life Safety is a term used in our industry to describe the systems contributing to the safety and care we owe to our guests, customers, and employees. A failure of our life safety system is not only a threat to the humans who rely on it but can be a liability for your company if it is not addressed.

Life Safety is also a state of mind or feeling that evokes both positive and negative emotions. A dark parking lot, for example, makes employees feel unsafe or even scared. A fire alarm that continually "falses" becomes an annoyance and therefore less effective.

We all know that a lawsuit filed after a criminal act on our property is less about the perpetrator or the circumstances and more about the conditions or physical safety measures that were in place or should have been in place to prevent it. It is our job to anticipate those acts and take action to prevent them.

A simple example is a dark parking lot. Our emotions tell us this is scary. Our experience tells us this is an environment conducive to criminal activity. These conclusions will be compounded if a violent crime actually occurs.

Let's say you have a dark parking lot and you want to request some lights. Your CFO might respond with agreement but may add that our parking lot has been dark for years and nothing has ever happened. You need to attack that argument on two fronts.

First is Risk: Risk, as we learned in Chapter 1, is measured by combining Likelihood and Severity. The likelihood of an assault in your dark parking lot will depend on your neighborhood, prior incidents, and physical conditions. Severity is subjective but is easy to measure when violence is involved. Burglaries (which will also be reduced by lighting) are not as severe as an assault or other act of violence. Therefore, severity, when humans can be hurt, easily gets a high score.

Second is the feeling of safety. Employees, who feel unsafe traversing your dark parking lot, are your best advocates. This does not mean you put ideas in their heads and tell them how at-risk they are going home at night, but it may mean tracking their comments and using them for your justification. Depending on your business, you may have documented comments from guests or visitors who will tell you they feel scared coming to your building after dark. This may even affect business or employee morale, so if possible get testimonials from your sales folks and Human Resources people.

The bottom line in this case is really not the bottom line. None of your executives want to have an environment where those in it are at risk or even feel unsafe. The Life Safety argument is compelling and effective for raising your request to the top of the wish list, so use it with sincerity. If your Life Safety request does not turn out to do all you promised, it will be harder to use it next year so make sure your facts are not exaggerated.

Saving Labor

Security is often referred to as a "non-revenue generating department." This is a simple distinction from sales and operations departments that spend money to make money. Since security's business model is more of a support function, the best we can do for the company financially is save it money by spending less. One of the simplest examples of this is to replace human functions with technology.

Most security managers will agree that, given the choice between a static post and an officer roving a certain area, the rover is more effective. Thus, many fixed posts have been replaced with gates and access control solutions. The cost comparison between humans and technology is usually a no-brainer. A 24/7 fixed post costs the company well over $100,000 per year, even at modest wages and no benefits. And of course, there are lunch breaks, sick calls, and training costs. $100k will buy a pretty respectable controlled ingress. This is not to say that technology is going to replace security humans but it sure is going to make those humans smarter, more effective and their work experience more fulfilling.

Speaking of humans, many industries have already taken this to the next level with robots. Warehouses, malls, even casinos have implemented wheeled computers that can do some of the more mundane or repetitive tasks formerly assigned to their human counterparts. Don't freak out. We have not reached Skynet proportions yet. This is about operating more efficiently with the tools our tech partners give us.

But wait, there is more. So, you replaced a guard at the door with a gate and a camera. There is still some savings to be had by using analytics to watch the camera for you. Your fleet of robots might require personnel to program, repair, download, charge, and analyze the data they collect—Artificial intelligence (AI) to the rescue. We are just getting good at this technology, but many managers are using AI to justify labor savings on a more advanced level.

Going back to our CapEx ROI justification…The method is still the same. If you are just stepping into this arena, calculate how much you spend on labor and subtract the cost of the new technology. Chances are, your labor savings pays for the capital in less than a year. This will be music to the ears of your finance folks who usually receive ROIs that are for a year or more.

Remember that a Capital request is like a loan from the company to your department. The company expects to have the loan repaid. Unless your request fits one of the other categories, (like Life safety) this applies to Security also. Purchasing a new gadget under the guise of "cost-saving" better be just that or you lose credibility. For example, if the officer who was replaced by the gate at the door is simply reassigned to another post, you better show that you are saving an FTE (Full-Time Equivalent) by not hiring for that other position.

Security Envy

When purchasing or implementing new equipment, there are three schools of thought among companies that determine when they will jump into a new technology. These decisions are based on wealth for sure, but also on risk mitigation.

Some organizations seem to have an unlimited budget for new technology, always positioning themselves to be the "Beta site" for an innovation. This costs them more money, but from a risk standpoint, it generally keeps them out of the legal woods. Litigation is generally targeted at "inadequate" or "negligent" security. It is difficult to prove either of those accusations against a company that maintains state of the art technology to protect its personnel or visitors. So, their savings (ROI) is on the "back-end" or in risk management.

The second group of technology buyers is the most common. These are the ones that wait until a "best practice" is established with the new technology. This buying strategy is circumstantial, often less expensive, and safer from a risk standpoint. It is circumstantial because most companies do not have cash lying around to try the latest gadget before it has proven itself. So often it is purchased later because that is when the capital is available. Purchases made later are less expensive because the price on technology generally comes down as it ages, even if just a year or so. Waiting for the herd to come up with an industry standard is safer because it is easier to defend in court if best practices were used as opposed to some new gimmick.

The final group of buyers are the ones who wait until everyone else has the technology and they climb on board more out of necessity. This may be due to a lack of capital or it may be because whomever is in charge wants to be sure that is the way the industry is headed. These companies save money initially in not making the purchase but may take a gamble on being the only one, or one of a few, in the market to lag behind the curve.

After the October 1 massacre in Las Vegas, we all waited to see how the hospitality industry was going to react as far as implementing new security measures. A couple of resorts immediately established armed response teams, search dogs, and hired off-duty police. The majority, though, waited for one or more best practices to develop before making drastic changes to their security posture. A little over two years after the incident, at least one hotel is going to install and staff metal detectors at their elevator banks. It will be interesting to see if this becomes the best practice that everyone will be "forced" to follow or if another technology will replace it as being more effective. And as it goes, the little guys with no capital budget for such things will be left vulnerable. Hotels across the country will, under pressure from the herd, take up this decision whether they want to or not.

What does all this have to do with ROI? The answer is, for major purchases that are going to change your security posture (like metal detectors) your capital request may depend on management's stance and where they want to be: Front of the pack, part of the herd, or bringing up the rear. Once you know that, make your request accordingly. "Everyone else has one so we should too." Not very intellectual, but a reality for many security directors.

I had a boss once who, whenever we discussed a new policy, or a large purchase, always asked the same question (and maybe the only question). What is everyone else doing?

Timing is everything. This goes for capital requests as well. We already talked about Life Safety, Labor Savings, and Best Practices being good strategies for showing a return on Investment. There are, however, some things you can do to help assure approval of your request.

1. Timing. Did you know that capital money is given out in quarters? (Not the shiny ones in your pocket, but the three-month part of a year kind.) Most departments will ask for money that will be spent as soon as the calendar flips to the new year. In an effort to save money, the corporation that holds and distributes the checks does so on a quarterly basis. This means that while all the money allocated for the first quarter may be ear-marked, the third or fourth quarter may have some unclaimed funds that are available for you. How are you supposed to know this? See number 2.
2. It's who you know. There is likely one person that controls the purse strings in your business unit. Not the GM or CEO, but someone such as a controller that actually receives and distributes the money to the departments. This should be your best friend. Take him/her to lunch, pout your lower lip and ask how this whole capital thing works. "How do I write a request that will get approved?" "What types of purchases get approved?" etc. This person will also help you with number 1 (above).
3. I am not asking you to pimp yourself out. But I always found that these folks wanted to help, especially because they understood that we security people are not always cut out for this administrative stuff.
4. Speaking of timing. Did you know there is often extra capital left over after each quarter? If the sales department put in a request for a $500,000 customer lounge and it only cost $450,000, that is $50,000 that will be sent back to corporate if you don't jump on it. You are correct in your assumption that you cannot use money set aside for a lounge to buy a security vehicle, so you need to be creative (but honest). How about asking for new cameras for that lounge (not $50,000, more like $5,000 but you can upgrade the rest of your video system and still be all about that lounge that was approved)?
5. Strength in numbers. One of the best ways to show a return on investment and get the stuff you want is to team up with another department—especially a revenue-generating department. Much of the security technology on your wish list has relevance to others in your organization and many of the things being purchased elsewhere in your building can be useful to you as well. For example, license plate readers have an obvious crime-fighting feature but perhaps another department could benefit from knowing when their best customer is on property. Same with

facial recognition. Video analytics are used by large retailers for loss prevention, but they also share this technology with Operations to monitor the efficiency of cashiers, customer buying patterns, and product placement. An access control system in your parking lot has been shown to reduce burglaries but it can also make a nice profit. The sky is the limit on these partnerships.

I had tried for years to get capital to buy an electronic key cabinet, but I was turned down each year as there were priorities more important. The next year I got together with one of the revenue generating departments who would also benefit from the cabinet. He said hell, boy, I spend more on paint in a month. Or some such exaggeration. The fact is that what was a lot of money for the security Department was a very minor purchase for the big department.

The Pitch

Preparing the request. If you have ever written a business plan, you know how to write this request. You will include all the information that you gathered previously, putting it into an easy-to-read format, with photos of what it looks like, charts and graphs that support your findings, and an executive summary.

Executive summary. This is a short, maybe one page, summary of the entire request. Just the facts so the decision maker can decide if he or she wants to look into it deeper. Be prepared to answer questions even though they are answered in your written material.

The pitch. You may go through this entire process, and it may be approved on several different levels until it gets up to the grand executive president of all things. You may be called to the office to plead your case. The president will nod his or her head in agreement. The president will smile and take many notes. He or she may ask questions and enter numbers in a calculator. Then, after you are exhausted and exhilarated from your most brilliant performance ever, the president will say, “You’re right. We need one of those gizmos. I agree 100 percent.” Then, “But we can’t buy one this year.”

The moral. Don’t expect to get to this level. There are many things they want to buy and many factors, besides security, that affect their decision. They may consider new televisions in the guest rooms or adding on a sports bar more urgent because it will increase profits. Without those profits, we may not make it through the year. However, they have validated your proposal and may put it on next year. Do not give up. Shelve it until next year and then try again.

That third paragraph happened to me, so sorry if I am little bitter about it. A couple years later, the facilities guy made the same proposal for the same reasons and was approved. I still owe him a drink, may God Bless his soul.

Security Revenue

Security is just a big business expense to most general managers. They do not like paying for it, but they know it is necessary. There is no reason why Security cannot contribute to the bottom line. You may already be pulling some of your own weight without realizing it. These are ideas to get you thinking. They might not be relevant to your place, but I bet you can think of more.

Restitution

Your investigators can cover some of their expenses by recovering losses from employee thefts. In Chapter 8, we discuss the investigations process and loss recovery. Loss recovery should be tracked and reported to your boss and the controller each month or quarterly. This will show positive income being generated by the Security Department. Otherwise, it is deposited in some miscellaneous operating account and lost in the numbers.

Court restitution is a different matter entirely as it is actual revenue instead of savings. When you make an arrest for theft or vandalism, have a prepared document ready to include with the arrest report detailing the costs incurred by your department in making this arrest. The unrecoverable loss in a theft, the items broken, and the property damaged all have a value. Then there is the cost of the arrest itself. Two officers multiplied by two hours equal another amount. Then there are administrative costs associated with processing the arrest. Writing the report, copying it, and reading it all have value. Total this and you might have a couple of hundred dollars that you will submit to the court as restitution. The judge may or may not honor all or part of it and you may not ever get any of it, but whatever you get is more than you would have if you did nothing. You also may speak to your accounting department as to whether they can "write off" these amounts as unrecovered losses.

Parking

Many hotels use an outside service to manage or at least enforce parking. They call a certain tow company to haul away a car and that company makes hundreds of dollars each time. Why not do it yourself? So, you don't have any tow trucks or a tow yard. That is okay. How about disabling the vehicle with a "boot"? A boot costs a few hundred dollars and keeps a vehicle from being moved. Then, your department charges the drivers when they return to their vehicles. This may not be advisable for your guests' cars, but it is perfect for employees of the office building next door or the nightclub down the street. If you have plenty of parking, maybe you need to think about charging for it per hour or per month.

Special Events

Your Catering or Convention Departments may have certain events that require physical security. Look at how those departments address this with their clients. Either they allow them to hire their own contract security company, or they assign you to provide this service. You need to assess the risk of having an outside company exposing you to liability on your property. Can you vouch for their training? What if they use excessive force on an intruder? What if one with a criminal record is caught in the storeroom with the boss's daughter? Consider limiting the security presence at these events to your own personnel, or at least to a company that you contract. Either of these options puts revenue into your department and gives you some control over the risk on your property.

Lost and Found

Unclaimed merchandise can really pile up in a large hotel. There are numerous ways to earn money from these items. First, you can sell the items to the employees in a "rummage sale." Second, you can actually sell many of the items on eBay and get a higher price. Lastly, you can donate the items to charity and collect a write-off. Ask the controller if the write-off can be credited to Security because your department did all the work. This is, of course, after a certain period of time and after all efforts to find the original owner have been exhausted.

Back-Charging

You may feel like the revenue-generating departments take advantage of having their own private security force to do things that they cannot or do not have the work force to do. Talk to your boss about charging these departments for these tasks. This will accomplish two things. First, it will add revenue to your bottom line. Second, because it adds expense to the other departments, they just might reduce their calls for service. Your department wins either way.

Please remember that some of these ideas have to be proposed in the right context or you might be thrown out of the boss's office. Think about it before you just hand a list to someone. I have been successful with all of the ideas presented here, but I presented them one at a time and sought buy-in from other departments beforehand.

JUSTIFYING SECURITY

We have probably all been in the meeting or received the memo to reduce our expenses by 5%. The hospitality industry seems to be the first to suffer when the economy is down and the last to recover when it rebounds. Unfortunately, a reduction in business volume or revenue does not necessarily mean a reduction in crime or the need for security. Also unfortunate is the fact that the boss may not see it the same way. He needs to see a cut across the bottom line and this means everyone—including you—must bite the bullet. It is your job to educate your boss on why you actually need more security during these slumps, not less. You may meet somewhere in the middle with no cuts and that is a good compromise.

Crime Rates

You need to arm yourself with some facts: In a down economy, criminals have to work harder. Their hard-earned stolen money does not go as far, so they have to increase their thefts. Financial desperation leads to new criminals. Those who may have just been scraping by may now be "forced" into stealing to make ends meet. Crimes of opportunity increase. Whereas before if someone left their keys in their car or their bag unattended, they were less likely to be a victim. Now, those opportunists are increasing in numbers and are more likely to take advantage of any opportunity given. We need to maintain a certain presence of uniforms and active security to prevent crime on and around our property.

Internal Crime

In a down economy, chances are that hours have been reduced, wages are frozen, and people are being laid off. Employees become desperate and some even justify their crimes this way. "The hotel still has business; the bosses are probably getting their bonuses, so it is only fair if I take a little off the top." They will become more creative, greedier, needier, and, if not stopped, will drive the business down even more. Cuts in security reduce the number of audits on these employees.

Guest Comfort Level

Everyone can feel the crime increase, especially when traveling. Guests want to get away from troubles like those described previously. When crime is up, Security needs to ramp up equally to provide the same level of protection that it did before. Guests are not necessarily looking for security but feel it when it is not there.

Terrorism

Don't forget about this threat that has been looming over us for decades. It has not gone away and is not likely to go away. Whether or not you see an increase in terrorism around you, realize you are not immune and you cannot let your guard down. One incident, no matter how small, even if it fails, can ruin everything. You may never recover from this loss of business and guest confidence. Reducing the staff that keeps this threat away is a huge mistake.

Making Those Cuts

Before the boss starts cutting salaries and laying off security officers, let's throw in some bones to keep him happy without hurting our operation.

Creative Scheduling

I know you probably do this already but take a hard look at your schedule. Do you need all those officers at all of those times? Maybe your patrol frequency ebbs and flows, and you do not need three shifts with the same number of people. Look at staggering shifts so that different start times allow for staffing levels to rise and fall according to the need for security during those times. Look into four-day workweeks of 10-hour shifts. See if this works just for your high-volume shifts to give you an overlap while the nightclub is open. Depending on the type of business you have, perhaps you are fully loaded on day, and swing and run a skeleton at night. You know your business. Just take a close look. Taking an inconvenient cut is better than a slash from the top.

Briefing

If you pay your officers for a pre-shift briefing, consider using this time for the operational duties of the department. See if the briefing can be done through email, pass-down logs, or even on the radio. Put pertinent information on a bulletin board and require officers to read it before starting work. I like the camaraderie and consistent information flow of a pre-shift briefing, but I would rather lose that than officers from the hotel.

Several lawsuits have been filed over the years by security officers claiming they should be compensated for time spent preparing for shifts and attending pre-shift briefings. These lawsuits, some of them class actions, have been decided in favor of both sides. The consensus is that officers do not have to be compensated for time spent on minimal activities preparing for work, such as putting on uniforms, obtaining their firearms, etc. However, briefings have been perceived as a work-related meeting and therefore compensable.

Getting ready for work is not unique to security officers and not an activity that most courts consider part of payroll. It is generally not fair to require workers to attend a meeting and not pay them for it. Check with your HR Director or legal counsel to ensure that your policies do not violate labor laws.

Supervisors

Look at the duties of your supervisors. If they are spending their entire shift in the office, there is something wrong. They need to be “on the floor” supplementing the shift. They can cover breaks, vacations, and delegate some of their duties to others.

Spending

You should look at cutting your spending before someone else does. Look at that current year budget and see where all the money goes. Copier repairs? Really? Do we need all those copies? How about radio repairs? New radios now can be cheaper than the repair on the old ones. Prioritize your spending into needs and wants. Then make the cuts yourself. Even 5% will not hurt you, but it will please the boss.

Procedural Changes

If you are still doing things the way you always have, there is a chance you can save some time and money by re-examining your procedures. Labor is the largest part of your budget, so what are those officers doing all the time? For example, if you have two door hosts and two floor officers in a small nightclub, perhaps you can have one of each and a third that watches both. That is a 25% cut! You also can start the night with minimal staffing and ramp up to full strength at peak time. Do not cut security where you need it, only where you do not.

Patrol Areas

If officers have time to stand around talking, they are either goofing off or their patrol area is too small. Try increasing the area they must cover. They should be on the move all the time, giving you good coverage. The boss will think you are over-staffed if he or she sees officers standing around talking while he or she is asking for cuts. In other chapters, we discussed how to set up patrol areas and whether to use physical patrol, video, gates, etc. Take a closer look and see if you really need that physical patrol in that area or if a camera can cover it as well.

Arrests/Reports

Arrests should be the last option when dealing with any situation. An arrest not only opens you up to liability for false arrest, but there are also injury claims (from the suspect and the officer) and they take up a huge amount of time and resources. Make sure your supervisors know that an arrest is warranted only if nothing else works. Be unreasonably reasonable with irrational persons. Even if your policy dictates calling the police, make sure this is the safest and most effective method. Reports also take a lot of time. Determine why you are taking the report. Remember that you are not a police department and you have no obligation to take crime reports. Your reports are to protect you and they do nothing at all for the guest. Burglary from a vehicle in the parking lot: You probably deny those claims anyway, so why do the report? Damage in the hotel hallway: You have no suspect and you will not. The damage will be repaired whether or not you write a report. Think of all the incidents for which you write reports and ask yourself what they are for. Maybe a log entry will suffice to have a record that the incidents occurred.

There are many ways to save money in security staffing. It is much better if it comes from you rather than an arbitrary across-the-board cut. If you make these decisions now, you can cut staff through attrition (people leaving on their own) rather than having to lay off employees.

10

Nightclubs, Restaurants, and Bars

Including a Contribution by Russell Kolins, CPP

Whatever you want to call yours: Restaurant, beanery, café, diner, eatery, grill, cafeteria, greasy spoon, hash house, chophouse, pizzeria, bar, watering hole, inn, pub, dram shop, cantina, gin mill, grog shop, saloon, taproom, tavern, alehouse, barrelhouse, bistro, brewpub, cabaret, roadhouse, speakeasy, honky tonk, canteen. They all have one thing in common:

ALCOHOLIC BEVERAGES

Any business that involves the service of alcoholic beverages is going to have risks. When these risks are not mitigated there is injury, death, and a financial cost to the business. If only there was a school for bar owners. I believe if most entrepreneurs understood the risks involved in opening a bar, they would not. In the many civil litigation cases I have worked and reviewed regarding alcoholic beverage service, I have seen the right way to do things and the wrong way. This chapter is about the right way of doing things that will keep your patrons safe and your bar out of trouble.

Alcohol is the main attraction at any bar or nightclub. The band or DJ is secondary. Without alcohol, your club would not survive. Be careful not to take the responsibility of serving alcohol for granted. It is a privilege, as your jurisdictional authorities may remind you with inspections, regulations, and fines. Keep your eye on the following issues to keep your venue "alcohol-safe."

Of course, a bar within a hotel or other facility applies those same risks to the entire organization.

Generally, this is why these types of bars operate at a higher level of safety, with less problems. The bad news is there are no standards and very few best practices documented for the safe operation of a bar. The good news is there are many governments, police departments, and associations that offer advice on the safe running of a bar. In addition to

DOI: 10.4324/9781003037644-10

our peers, we have the experiences and mistakes of 250 years of alcoholic beverage service to help guide us. And that is just in the US.

What follows is the compilation of those best practices, experiences, and my own experience on how to manage the safe operation of a bar or nightclub. Imagine your local pharmacy allowing its employees to consume some of the drugs that they were dispensing. Suppose your pharmacist bottled up your 30 opioids, added three or four more because you are a good tipper, and then took a couple for himself because he can. I am exaggerating to prove a point. Alcohol has similar and as harmful effects as some of the most dangerous drugs you can receive with a prescription. Yet we are much looser with alcohol than we are with drugs as far as providing it to our patrons. In fact, we do not allow our pharmacist to be intoxicated while dispensing drugs or to dispense them to intoxicated persons. We also do not condone patrons consuming those drugs on pharmacy property. I think you get the idea.

I also suspect you have seen bars that are pretty loose with the rules and careless with their dispensing of this dangerous drug, alcohol. I am not intending to come off as prude, but I have seen what alcohol does to people, including those that do not drink, and I have seen what bar management has done or has not done to prevent some of these horrible things.

First, let's get the terminology right. When I mention "Alcohol" anywhere in this book, I refer to alcoholic beverages. "Alcohol" by itself is a disinfectant. Where there is alcohol, there are generally drunk people. And when you have drunks, you need security.

Nightlife Security (Nightlife is a term I use for most of the establishments we are discussing) has several vital functions that help make our adult venues successful. From the vetting of entrants at the door to keeping the dance floor free of safety hazards, our security officers contribute directly to the operation. This document outlines training, duties, requirements and the "do's and don'ts" of operating within acceptable bounds.

Alcohol

Training—Everyone who serves or deals with alcohol in any way should be trained in responsible alcohol service. This training includes recognizing intoxication levels, proper cut-off procedures, ID recognition, and how to deal with intoxicated persons.

Over-pouring—Bartenders and drink servers can make huge tip money that can affect their judgment. Make sure your policy on serving to patrons and potentially intoxicated patrons is enforced by Security and management. If they know that their job is in jeopardy, they are more likely to follow those policies.

Minors—A minor being allowed entry and then served alcohol is likely your greatest liability. Strong policies, such as checking every ID, are recommended. This takes the heat off the bartender and server who are motivated by tips. If you come across a minor who is intoxicated, make sure you turn him or her over to a responsible adult or the police. Putting him or her back on the street just increases your exposure. Document these situations very carefully to show you acted reasonably and responsibly.

Intoxicated persons—Everyone in a bar or nightclub has some level of intoxication. The club should have a liberal designated driver policy. Providing free coffee and soda to designated drivers is cheap insurance. Beyond that, your staff needs to be aware when guests have reached their limit. Some behavioral recognition skills come into play and are taught in awareness classes. Absent that training, reasonable judgment needs to prevail. Someone who cannot clearly speak, walk, or make simple decisions is past his or her limit.

Security serves many purposes in a nightclub/Bar. We will review all of them, but first, we need an objective. The number one job is guest safety. There are many safety hazards in a bar, including alcohol, of course, but also fights, falls, drugs, stalkers, crowds, minors, and even bouncers. Let's talk about a few of these and then we will dive in.

Bouncers—Of course we still use this term, but the practice is a bit outdated. "Manhandling" someone is no longer accepted by witnesses with cameras, police, and the ones being manhandled. Gorilla-style security is no longer the common practice and it is a huge liability for the gorilla and the owner. I will have some alternatives coming up in this chapter that you can use to keep your guests and your employees safe.

Fights—You may be surprised to learn that alcohol does not start fights. It is fuel for the fire, as they say. Fights can be avoided, and we will talk about prevention and intervention.

Accidents—Alcohol affects balance, so falls are common in bars. But there are other factors such as crowds, lighting, and difficulty to clean. Accidents will account for many of your insurance claims and can cost you much more than a fight.

Drugs—Drugs make their way into every establishment, regardless of your demographic. Party drugs such as Extasy and Molly are common additives to having a good time in a club. Roofies are still associated with sexual assaults. Marijuana, heroin, crank, and others are common everywhere. Then there are opioids, which are as prevalent as beer in a bar. We will talk about some ways to prevent some of this traffic in your place and how to deal with its aftermath.

Stalkers—Did you know you have guys waiting outside your bar—and inside—for intoxicated females to come out alone? They may pose as a boyfriend or a rideshare driver or a friendly citizen. Many women wake up Sunday morning not knowing where they are or what happened. This may be partly on you if she got drunk and walked out of your place in an unsafe condition. We will review ways to deal with this.

Crowds—Crowds are a good problem to have, as they say. The owner markets to bring in volume and then once you have it, there needs to be control. We will talk about staffing numbers, deployment, crowd control, line management, and everything one needs to know to handle lots of people.

Minors—Most of the citations written in bars are for serving minors. This is on you and not the minor, in most cases. Diligence is not good enough and rarely enough of an excuse. Looking the other way is no longer an acceptable practice and it just takes one employee to ruin your business. Imagine the worst-case scenario—perhaps a minor leaves your bar drunk, drives her car the wrong way on the freeway and kills herself and a carload of others. Her family will own your bar, your house, and those of your responsible employees. You do not want those deaths on your conscience, so we will talk about doing the right thing.

Guest Service

Those of you waiting for the butt-kicking part of this chapter need to wait a bit longer. If you have read other parts of this book, you know that security starts with good guest service. Many companies have a theme such as "be our guest," "family-style," or white glove service. Whatever your company's theme, you need to train and hire your employees to use it—all of your employees.

Experienced security officers soon learn that a friendly demeanor helps to prevent violence and diffuse difficult situations before they escalate. In security, we view that friendly demeanor as the first tool in the de-escalation process. A badge-heavy officer with no social skills may regret these negative interactions when a crowd turns on him during a fight or other incident.

This is just good business. Have your employees treat each patron as a guest who has gotten dressed up, driven a long way, and arrived at your home for a party. How would you welcome your friends at the door? You would make sure they were not already drunk, dressed appropriately, and then invite them in. You would address them by name and offer them a drink. Some variation of this style sets the tone for your guests and will come in handy later.

When hiring doormen (bouncers, security) we tend to look at their experience as bouncers, their muscles, and do they resemble a TV wrestler. I suggest you make those traits secondary and hire those who have good people skills.

Another trait that should be secondary when hiring is the younger male. Many of these guys become bouncers for two reasons. One is their desire to fight. These guys can be trained and told and nagged and they will still endeavor to use their new moves on the next aggressive inebriate in your bar. Speaking of "moves" that brings me to reason two. To a young male bouncer, a nightclub queue line is like a buffet of women. While some flirting is expected and within reason, distractions and conflicts are not good. Fighters and flirters is a generalization, but it fits the majority of your applicants. Just use caution and keep this in mind. Relatives of management may be against your better judgment as well. Be careful of those who will let in their friends, brag about their authority, or be less diligent because it is below them.

Good people to hire are mature men and women who may be retired cops or teachers or bartenders. Young women should not be overlooked, as you need women for many of the duties we will be performing. Mature women can de-escalate better than anyone.

I am not disparaging any one in particular. My generalizations are for comparison. Never discriminate based on gender, age, race, or any other protected class.

TRAINING

Training is laid out in the training chapter so here we will go over some things unique to nightlife security.

Training Topics

Guest Service. Of course. Enough said.
Basic Criminal Law—Trespass, burglary, theft, and alcohol laws in your jurisdiction
Arrest Procedures—Laws of arrest as well as the physical procedures
Defensive Tactics—Those who come to you with martial arts or military training will have to be re-trained. None of that here.
Alcohol Awareness—Security should go through a state-mandated or state-recommended training program whether it is required for your license or not.
ID verification—Security will need to know how to spot fakes, trades, and stolen IDs. This is your first line of defense against minors as I wrote above.
Company Policies—Whatever policies and procedures your establishment may have should be written and shared with each employee. If you need ideas, stay tuned.

No matter how small your operation, this will require some classroom, or sit-down training. You cannot explain arrest law on-the-job. On-the-job training tends to get diluted in real life. We hire someone because we are short. We get them on the job, and we do not have enough people to shadow the new person around. No matter how hard it is, I urge you to do it. In the absence of correct training, bad habits set in. This can cost you with use-of-force, bad IDs, and de-escalation.

Appearance

The attire of your staff sets the tone for the entire establishment. A formal look (like a black blazer and black pants) conveys a reputable place where violence is avoided, and people treat each other with respect. A casual look (like t-shirts silk-screened with "security") tells people that we have muscles, and we aren't afraid to use them.

I would suggest the formal, or at least something in between the two examples. A collared shirt is better than a t-shirt. There should be some uniformity and something that identifies the wearer as Security.

Here is a sample of a policy you could use for your staff's uniformity.

Nightlife Security personnel are expected to look their best when representing the company on or off duty. Uniforms may vary depending on venue, but those items not provided by the company should be clean and in good condition. The following basics apply to everyone.

- T-shirts are not permitted unless worn under the visible shirt.
- Shirts with buttons must have all buttons fastened except the top button at the neck. Properly pressed and tucked into the pants.
- Hats and caps are not permitted.
- Name tags and a lapel pin, if provided, must be worn and visible at all times. No other pins or insignia may be visible.
- Jewelry must be worn under clothing, where applicable.
- Pants must be tailored slacks, with a belt at the waistline. No jeans or cargo pants allowed.
- Shoes must be all black leather or similar. Cloth, canvas, suede, and the like are not permitted.
- Socks must be black.

Personal Items—Purses, backpacks, and other items not required for work must be stowed back of the house in an office or locker.

Tools—Only those items provided or authorized (radio, clicker, flashlight, etc.) may be carried while on duty. Weapons of any type are prohibited. A utility knife with a blade no longer than 4 inches, single edged, is allowed but may not be used as a weapon under any circumstances.

Grooming—This aspect of appearance may have to be varied based on the type of club and music. Here are some considerations. Neatly cut, clean hair (long or short), neatly shaved beard, and personally clean conveys authority and commands respect better than its opposite (when combined with a positive attitude). So the good news is you can have some leeway for those with long hair, piercings, tattoos, and beards, but keep it neat, clean, and between the extremes.

Shared Labor

I have seen so many places, especially smaller ones, or those with limited staff, use barbacks as security officers, or some similar arrangement. This is not recommended because it creates some holes in your security system.

Instead of finding things to do for security officers that seem under-utilized, bolster your security. If you have a security officer that appears to be doing nothing, he needs some motivation. Train him if you can, or trade him in. There is plenty to do in a bar, even if it is quiet. You and I know that the officer needs to be using his five senses to monitor this post and be ready to de-escalate a situation or clean up a spill or watch intoxication levels. Nevertheless, a bar manager who sees a security officer sitting around, is likely to repurpose him. If you have two doormen and one keeps getting called to change kegs in the cooler, who will be held responsible if a fight breaks out, someone slips and falls, or walks out drunk. Both need to be on post, visible, and vigilantly looking for signs of violence and safety hazards.

I also discourage assigning security officers to duties like taking money at the door for a cover charge, selling the t-shirts, or even selling bottle service. Again, how can they watch for safety issues if they are counting money? If security officers are watching for theft, who is watching security? Keep them neutral and away from money.

HOUSE POLICIES

Age Requirements

In 1984, Congress passed the National Minimum Drinking Age Act. It required states to set their drinking age at 21. This has been about as effective as a speed limit because 11% of alcohol consumed in the US is done by those under 21 (according to the Centers for Disease Control).

I give you this information for two reasons. First, you should always have or demand context for why a rule is what it is. I think we can all understand why the drinking age is 21, but if you do not, here are a couple more facts for you.

- Thirty percent of teenagers have had a drink in the past 30 days.
- Excessive drinking is responsible for more than 3,500 deaths among underage youth each year.
- Underage drinkers consume more alcohol than adults per session (binge drinking).
- The Human Brain (at least the part that controls reason) is still developing as a teenager.

The second reason I give you this information is that those statistics put the focus of many anti-alcohol groups on your bar.

Did you know that most enforcement actions performed by the police are grant-funded? Police operations that are outside of their normal duties, like DUI (Driving Under the Influence) checkpoints and minor stings, are paid for by the Federal Government and private groups that are against alcohol and drug abuse by minors. When the police or code enforcement find an employee allowing entry to a minor or serving the minor, the citation goes to the employee. This is probably the only violation in your business that is directed to the individual. But wait, the business is not innocent, so when they cite your employee, a copy is going to the agency that holds your liquor license. That entity may give your business its own citation, which of course puts a threat on your license and your business.

Fake IDs, mistakes in calculating age, and distracted employees are not an excuse for allowing a minor to purchase alcohol. If a police officer or a code enforcement officer cannot find a person responsible for serving the minor with a drink in his hand, he will cite the business instead of the employee.

If you are just the security guy and not the bar owner, then consider where you will be if one of your people is responsible for the loss of revenue caused by a suspended license. Even worse, you and your staff do not want to be responsible for a minor who is involved in a catastrophic accident due to being drunk. OK my lecture is over, but frankly, your 21-year-old employees are not as easily convinced. Strict policies and enforcement of them is your best chance of managing this important issue. That brings us to Identification.

Identification

Your state or local government may have certain requirements for acceptable IDs. Some states allow foreign IDs or IDs from private organizations. Make sure you are compliant with these guidelines but also remember that we are not checking for citizenship or anything else. Just age.

The altering, forging, and manufacture of IDs that misrepresent age are abundant and probably always will be, but just like counterfeit currency, the government keeps stepping it up and trying to make it more difficult. As of this moment, we have some pretty good safeguards on our IDs that require alert and knowledgeable employees. In 2005, Congress passed the REAL ID Act. As of 2020, all states had become compliant with the requirements of this act, which ranged from recognizable authentication features to the requirement of certain documents to obtain the license. This is good news for us ID checkers because it means MOST people will have an ID that is easy to authenticate.

First, you need a policy on ID that includes what types of ID you can accept. For example, the Transportation Safety Administration will only accept REAL ID compliant IDs. But there are foreign IDs and IDs you buy on the Internet that are less genuine. Then there is a foreign voter ID card, certain consular cards and tribal IDs that are difficult to authenticate. Some people that can help you decide what to accept are: your legal team and your local police. The other part of your policy is who gets carded? Everyone? Persons who look under 40? 30? 25? Don’t worry too much about offending the 30-year-olds. If they have ever been anywhere, they are used to it. Just tell your staff to blame it on management.

Once you have decided which IDs are acceptable, you must train your team how to spot a genuine ID. Every ID has discreet features such as micro-writing, holograms, and unique material. Your state website will tell you the features for your cards. It is good to get a reference guide that has the IDs from all 50 states and some countries so you can check those. Software is also a solution and I will go over that soon. One trick for minors is to alter an ID from another state that you may not be familiar with. Once your team works a door for a month, they will be experts.

REAL ID, as I mentioned, is a bit more secure and updated with modern features. The good news is that all states are now compliant so if you are dealing with a 21-year-old, chances are they have a Real ID. If they do not, it is worth a second look. You will also see many International Driver’s Licenses. Yes, there is such a thing, but they are rare. If they are a US citizen, they have to get their International ID in the US, so if they present an International, ask where their DL is. They are either underage, or they gave it to their sister or roommate who looks enough like them. If you have a foreign national who presents an International Driver’s License, I would not accept it. They should have a passport or Visa. The main problem is, you can go to many websites and order one in the mail. The only place to get one in the US (that is legal) is the American Automobile Association (AAA) or the American Automobile Touring Alliance. If you see one not from those places, it is bogus.

Mexican IDs are problematic. Not to pick on our neighbor, but they are our neighbor, so we …see plenty of their IDS. Mexico uses a Voter ID as a National ID since many Mexicans do not drive. These are legitimate IDs, but I have seen more forged ones than real ones. The Mexican Consular ID is also a legitimate card that is issued by Mexican consulates outside the US. As you might guess, many illegal aliens get these cards because they do not require significant supportive documents. But we are not here to get political, just to verify age.

Some other IDs you do not want to accept:

- ID cards from foreign nations (except Canada). Foreigners should have a passport
- Any ID that is damaged or unreadable
- Paper documents from DMV
- Expired ID
- Altered (in any way)
- Photos or facsimiles of ID
- Known persons with no ID

People will take a photo of their ID and show it to you on their phone. Most are doing it to avoid losing their ID, but unfortunately, we cannot tell if it has been altered or "shopped." The newer polycarbonate cards have mostly eliminated the wise guy who folds his license right on his DOB (date of birth) so you cannot read it. Crossing out the address and writing a new one also has good intentions but makes our job harder so I would not accept it. It is illegal in most states anyway. Some doormen will get so focused on deciding if an ID is genuine, they do not even look up to see they have a 40-year-old standing in front of them. Remember, it is about the age, not the ID.

While we are here, I want to talk about the laws that prohibit minors from drinking. Here are a couple of details.

- Many of these laws are written by your city, county, or state.
- They write the law very generally. Meaning there may or may not be a law about faking your age, presenting an altered ID, or even entering a bar.
- Most laws simply prohibit providing alcohol to a minor. Most states do not have laws about minors consuming alcohol or being intoxicated. The law is aimed at you.
- So that is good news and bad news. Good news is that, by law you do not have to check IDs or be held accountable if you sneak your 22-year-old in without an ID.
- Bad news is that if someone gets past you, regardless of whether they had a good ID or a bad one, the crime will occur when you serve that minor a drink.

Check the laws that you have to follow because you may have a law preventing minors from loitering in a bar or being intoxicated or presenting a fake ID.

There is some technology that helps us with ID checks but let's go over it manually first. If at all possible, you should have a security person at the door checking IDs. If you are working a small tavern, such as that with a bar and a couple high tops, and one door, then you may not need it, but it does take heat off of the bartender to be checking IDs. This does not give you permission to do without security because you are small. I am also not saying that your bartender does not have to check IDs. Remember that the citation is going to her if she gets caught selling alcohol to a minor so she should have a policy to on which to rely that gives her latitude to do a second check if she has any doubts.

Depending on the size of your venue and the volume coming in the door, it is good to have a second person at the door. Posts are discussed later. The single door host has many responsibilities so let him take his time to scrutinize the ID, look at the bearer and then do all of the other things we will require of him. The process should go something like this. Greet the guest (discussed later but remember this most important step). Refer to your policy as to who gets carded. If we are checking manually, most places use age 40 as a cut-off.

Hold the card in your hand. Of course, someone with a fake will want to hold it so they can pull it back when you make that face. Also, if it is in a wallet behind a plastic insert, you may not see its flaws. First, feel the material. Most IDs now are plastic like a credit card and not laminated paper (states differ so check). Next, look at the photo and compare it to the person. They should be very close. Unlike your mother, who took her DL photo 20 years ago when she was blonde, we are dealing with 20-somethings who have not been alive long enough for their photo to be outdated. Look at the eyes, nose, and chin. Hair obviously changes. If there is some doubt, refer to your policy or manager as to making a judgment call. This holds up the line, so let someone else deal with the patron while work continues. Another solution is to ask for a second ID, such as a student ID or even a credit card that has their name on it.

That was just the photo, next look at the birthday (make sure you can do the math). Forget about the stupid questions about their zodiac sign or zip code. That does not work, and it will not be a defense for you if you get a citation. The ID either matches or it does not. Refuse if you have some doubt. The oldest trick in the book is to alter the year on the DOB. So of course, check that. My state uses laser printing which makes that quite easy to spot.

Then use at least one of the security features to determine if the ID is genuine. Many doormen prefer to have UV flashlight to see the UV writing on the card. This is a good one, but there may be others. A simple scam is to take a genuine ID and put a fake picture on it and laminate it. That will pass the UV test, but if one is paying attention, it will look obvious.

This process will be slow at first and become quicker as your staff gets to know IDs. Some venues are restaurants in the evening and then transform to a club later at night. If so, there will be minors allowed in the restaurant during those times. It does not make sense to check IDs at the door in this situation. Like any restaurant, have servers check IDs and then when you switch over to nightclub mode, you set up at the door. During that transition time, check the restaurant for minors and make sure they leave or get carded after food service ends.

Crowd Manager

In 2018, the International Fire Code added "crowd manager" (CM) as a required job duty in every place of assembly (that includes bars, clubs, theaters, meeting rooms, casinos, and just about everything). This code, if it was adopted by your local authority requires a trained crowd manager for every 250 attendees. That math works out fine for us. We have a much lower ratio than 250:1, but we do need to make sure we have our CMs trained and certified. This can be done online, generally.

A CM is responsible for the safe evacuation of patrons in the event of fire, alarm, active shooter, or any other emergency. I completely agree with the training and the requirement and all security personnel should be certified. I have a few examples throughout the book where evacuations failed horribly.

VIPs and Known Persons

A successful nightclub will have a certain number of VIPs. These are people known to the club, who spend a lot of money, or are just plain good looking. The club likes them for their money, but also because they attract others who spend money. Depending on your policy or the discretion of the manager/owner, you may have to break the rules for these folks. For example, if the town college basketball star shows up with a logo track suit (which is against your dress code), you will likely be told to let him in. This is not up to me, but you need to work this out in advance with your boss. Other discretions you can expect:

No ID—If someone in management is willing to vouch for him, there is no law requiring ID—just age. Well, sometimes there is a law, so make sure.

Ladies with inappropriate clothing—I have seen club managers walk outside, grab the two most beautiful women wearing hardly anything and invite them in for free. This is a business after all, and pretty ladies attract men, who pay for drinks. Once you figure out what the manager wants, you can do this yourself which will save you embarrassment if you would have turned them away. We all know a pretty woman can start men fighting. That has been a fact of nature since Helen of Troy and before that. Make sure you know the theme or the intent of the club management. Before stepping onto this slippery slope, talk to management and see what crowd they want. If they are looking for a Vegas or NY style club, then spaghetti straps are the way to go. If you are catering to blue collar Friday-after-work crowd, then a bit more conservative might be better. And heaven help you, your demographic is hip hop and rap, they will wear nothing and have sex on the tables. I am exaggerating to prove a point. Do not assume that the same dress code or appearance applies to every customer.

Tips

Gratuities are a difficult part of managing a club. It is normal and expected for a door host to get a tip for letting someone cut the line, or from a VIP, or to circumvent the dress code. It is your property—do what you want but take these cautions.

Doormen will set up their own enterprise at the door, holding the line until someone approaches with cash. That may be OK, but it causes management two problems: It cuts into revenue. The five people, who could have gone in while the line was held, do not have their wallets out. The guy that tipped the door host is going to expect something in return. If he has a problem with another guest or employee, or gets kicked out for being too obnoxious, then he will expect you to back him up. I am not saying to do it, but you need to be prepared and have a policy.

Make sure that the acceptance of tips is not in lieu of following a policy or law. For example, here is 20 bucks, can my kid sister come in just to look around. That is against your policy and he should not accept the tip and should not let her in. Draw your lines, set boundaries, and enforce them with your staff.

Depending on your hierarchy and the tenure of your security staff, they may want to keep their own tips—or pool them. Both ways have pros and cons, so let them decide. Here I come with bad news again: Ask your HR people about pooling tips. The Internal Revenue Service has been around in the past cracking down on food and beverage service employees who did not report tips. Pooling tips documents the amount, and what may be a low IRS estimate of tips received, may become an actual number.

Bottle Service

If you do not have a club, you may not know about bottle service so let me explain. VIPs may come in—or make a reservation with someone they know at the club—and arrange for a table. They purchase a bottle of the good stuff and depending on the venue, and the day of the week, is anywhere from $300 to $3,000. Now someone that can buy a bottle of vodka for $1,000 is not just drinking at that table. He will bring his own entourage and then he will pick up ladies in the club, who are generally delighted to be asked to the table. Sometimes these tables are booths and may be curtained off. That is where you may have your problems. I am not talking about the sex, drugs, and illegal activity taking place behind the curtains. The problems you will have are wanting to eject that party for the nefarious activity and your club manager only sees dollar signs.

Besides the money, you may have an owner manager who thinks that drug-induced, drunken, consensual sex is perfectly fine on private property. Your problem, then, may be with your liquor authority.

In Nevada, the Enforcement Division for the Gaming Control Board was receiving complaints that a casino nightclub was ejecting drunks out the back doors and causing a nuisance and a mess for the taxis. The Gaming Control Board regulates every revenue center in a hotel/casino but had traditionally stayed out of the clubs. But this time, they used their authority to do some undercover operations and learned quite a bit. This nightclub and many others were engaged in drug use, drug sales, prostitution, and human trafficking. That was bad enough, but the staff including security were taking money to look the other way. There was a huge fine and a big black eye for all the casinos that had clubs. Nevada laid down some strict oversight rules after that.

The short story is, find out what is happening in your club, get with your management and see if it is all legal and something they want. If you disagree, then make your own decision. In my opinion, supporting illegal or even borderline activity not only puts the ownership at risk, but damages my own integrity so I would have a hard time with it.

Back to reality. Let us look at some of the bad things that happen in a nightclub. Bars and Restaurants will have their own sections.

Prohibited Activity

Do not be naïve about the behavior of your guests when you put them in a dark room with booze and girls. This is a choice the club makes. You make up a booth, put curtains or whatever around it, supply it with high-priced liquor and a beautiful server. What do you expect? If that is what management wants, management will have to decide what they will allow. Looking the other way does not work anymore. The law enforcement attention to trafficking, drugs, and liquor violations are too great.

So, get that worked out with management. My recommendation would be to have bottle service but reduce the environment to one that is not closed off. Make drugs zero tolerance in there and no sex in the booth!

Besides the drugs and sex, this is an ideal place for gangs, pimps, and organized criminals to set up shop and establish turf. We do not need that kind of customer. If some bad stuff happens and you knew it was going on, the club will be closed forever.

Dress Code

Properly dressed patrons determine the image of the venue. More importantly, attire can be provocative, indicative of criminal or violent behavior, or in extreme cases, physically threatening. Each venue may have variations to their dress code depending on the environment that management is trying to achieve. Each attire rule is explained here whether it is prohibited in each venue or not.

1. Headwear—Generally all caps, hats, and hoodies are prohibited. This allows cameras and employees to see a person's face. This also contributes to our image: A respectable establishment discourages headwear, especially by men.
2. Jackets—Except for sport coats, jackets should be checked in (if available) or left in the car or a coat room. Jackets tend to get removed soon after entering the club and create additional hazards. They also cover other clothing that may not be allowed. Jackets conceal weapons, bottles, and other products not permitted. Sport coats should always remain on the person.
3. Tank tops, tube tops, spaghetti straps, and similar articles may be excluded at the discretion of management.
4. Logo shirts and tops—Writing on clothing is subjectively provocative so rather than decide on each item, we generally prohibit anything that has writing, a message, icon, or logo on it. Even sports names and colors can have gang associations. These include profanities, gang symbols, violent-provoking messages, and nude images.
5. Pants—Pants must be worn from the waistline to the ankle. Exposure of underwear or skin below the waist is inappropriate. Persons who volunteer to pull the pants up to enter should still be refused because they are likely to come back down once inside. Pants with rips or openings that show genitals, or the buttocks are not allowed.
6. Shoes—Rubber or cloth (sneakers) shoes are generally not allowed. Shoes must have soles and cover most of the foot. Sandals not allowed. The discretion used with shoes is based on whether the shoes are safe to be worn in a dancing environment.

7. Sweatpants and suits, track pants and suits, pajamas, and similar casual clothing are not allowed.
8. Clothes and jewelry that are sharp, studded, or a safety hazard are not allowed.

Some of these may be too strict for your establishment and that is fine, but you will find fights and other problems are drastically reduced the stricter your dress requirements. Be careful not to discriminate based on race with your dress code. Apply it evenly and fairly. Avoid angry patrons by posting your dress code. If you have a line, post it at the end, not the front. How angry would you be if you waited an hour only to find out you were dressed wrong? We will review some other techniques for enforcing this in the "Posts" section.

Dress codes are subjective, so you need to make it simple and give someone power to override. By override, I do not mean we let our friends in dressed poorly, but I mean a manager who can size someone up and predict whether their entry is a good investment.

You will have someone each night who wants to argue that his sweatpants cost $300, for example. It is private property, and it is up to you, but consider your business. On clothes you can discriminate as long as the people wearing them are not discriminated upon. If you get someone who becomes aggressive and wants to get physical because you will not let him in, then you know you made the right decision. Do not give in to someone who is violent.

Prohibited Items

There are some things we do not want in a bar or nightclub. My list is here. If you come across something I have not thought of, ask yourself why they need that item in our bar.

- All weapons including pocketknives—many women carry pepper spray or electric stun guns. These can both be huge problems. Do not make exceptions.
- Sharp objects—scissors, forks, etc.
- Battering objects—any blunt instrument (including bottles of anything).
- Outside food and beverage—first, we are selling food and beverage. Your stuff has not been inspected by the health department. Second, we don't know if there is alcohol or drugs in that big gulp. No exceptions.
- Aerosol or spray cans or bottles with any contents—this stuff is dangerous and has no place in a club.
- Glass—safety hazard
- Clothing with sharp or dangerous attachments—spiked jackets, chains, etc.
- Backpacks, duffel bags, luggage, tote bags (purses ok)—what purpose do these serve? They are likely to get stolen and/or carry contraband. No way.

Note: You may want to periodically check the bushes, planters, trash cans, and other hiding places outside your establishment. You will find knives, pepper spray, and all sorts of things.

Searches

This is not a decision you make in one day. Searches are based on a risk assessment and the probability of persons bringing weapons or other dangerous items into your establishment. They are also not a magic bullet—so to speak. Searches need to be combined with other layers of security to be effective. I am not going to tell you whether you need to search—that will depend on your location, your staff, your music, your hours, and especially your past history.

> I had a case once where the owners purchased a bar from another company. The new owners failed to do a risk assessment. If they had, they would have found that the previous establishment had fights inside and outside, hired police officers to work the door and used a walk-through metal detector to discourage guns. That place had a shooting in the parking lot, which motivated them to close and open elsewhere. The new owners removed the metal detector, removed the police, and within a year had a murder right outside their main door. That bankrupted them as well.

Some considerations for metal detectors—Walk-through detectors are best, but more expensive and take more space. Exceedingly difficult to manage and may take more than one person. Detector wands, because they are generally misused, are not effective. It will be detrimental to have someone get through with a weapon and post it on social media. Metal detectors slow the line, which costs money, but your competitors are doing it, so you may not want to be the last person on the block to have one. If something happens at your place, uncomfortable questions will be asked. If you use any of these devices, make sure you use them on everyone—or it is a waste of time.

Physical searches—I do not recommend laying your hands upon anyone unless you are arresting them. This is an invitation to sexual impropriety, invasions of privacy, and discrimination. Look at the problems TSA has, and the strange procedures they follow to avoid complaints. One club I knew, did not like metal detectors, so they had the males who entered raise their shirts and show that they carried no waistband weapons. They caught a couple of guns here and there, and they did not get complaints of inappropriate touching or discrimination, but it is not 100% effective. Better than nothing, I suppose.

Bag Checks—This is a good idea no matter what else you do. Since you only allow purses, no backpacks or duffels, it will be mostly ladies. Ladies tend to take only that purse big enough to carry their wallet and some light make-up. So, these checks are fast and simple. Instruct your patron to open their purse so you can see the contents. We are looking for the prohibited items listed with our dress code. If you have blind spots within the purse, have them move items around for you. Never stick your hand into a purse. Clubbers are used to this process and will make it faster.

Decide what you will do with prohibited items before you come across one. Again, I would take a hint from the TSA and have the patron throw it away. Do not throw it away yourself; that looks like confiscation, which looks like theft.

Coat Check—Believe it or not, a simple coat check is a big hassle. You need an employee to monitor it and you will have loss claims every night. I had money in my pocket, you gave my coat to the wrong person, there was a belt with this. Then it turns into a purse check and everything else. I do not recommend it unless you are trying to up your level of service and can afford it.

By the same token, never ever check in prohibited items like knives, backpacks, and whatever. That defeats the whole purpose of having no weapons. Same with those ladies that will ask the door host to watch their purse. Once you take possession of something even if it's for a bathroom run, you risk a false claim.

Weapons

Guns will depend on a couple of variables. If you live in a state where open carry or concealed carry is common and legal, you may want to advise the patron to put it in their car. They are not criminals. If you have the opposite laws, you may want to report concealed guns to the police. No law says you have to report a crime or arrest anyone and I suggest you do not get caught up in this kind of arrest. Just because they have a CCW (concealed weapon) permit does not mean they can bring a gun into a bar. Private property trumps gun laws so make no exceptions.

Illegal weapons are similar in their disposition. Do not touch or keep an illegal weapon. It is just as illegal for you to have it as for them. Daggers, switchblades, Tasers, nunchakus, and other weapons determined by your state to be illegal should go in the trash. If the person walks away, call the police, and go about your business. Ban that person using whatever means you use. We do not want someone that endangers our other clientele.

As for pepper spray, stun guns, pocketknives and other legal but prohibited weapons, most people (ladies, usually) would rather toss them in the trash than return to their car, so let them. Do not dig through the trash in front of your guests. Keep in mind that the lady brought that weapon to get to her car safely or to keep scoundrels away, so you should have a way of ensuring their safety at closing and we will go over that later.

Police—This is a real quandary for some of us. On duty police officers is a given. Of course, you want them doing a walk-through whenever they can. But what about your local officers who come to your bar after work? Will you let them carry their weapon in the bar? Do you want them carrying a weapon while intoxicated? If it were me, I would allow it. I would not expect a police officer to pull his gun in a fight, but if you do have a problem, his buddies will usually take care of it and if they do not, a call to his supervisor will take care of it. You need to draw a balance with policy and good relations with law enforcement.

Out of town police get a different treatment from me. I would not let them in my bar with a gun. If they are not locals, then they are there for vacation or visiting and need to play by the same rules.

Drugs

Controlled substances have been an issue in clubs since Studio 54 in New York glamorized it 50 years ago. (We could probably go back further if we wanted.) Your patrons come to your club for a variety of reasons. One of those is to consume drugs and another one is to provide drugs. This generation of 20-somethings (they are not the only generation, jut the current one) likes to binge until they pass out. To do that on alcohol in a club would take too long and cost too much. So, they either "pre-game," meaning they drink at home or in the car on the way, or they supplement the alcohol with pills.

For the pre-gamers, it is important to screen intoxicated persons at the door. Drugs—not so easy. The choices right now for party drugs or club drugs are GHB (a downer called gamma hydroxybutyrate, MDMA (methylenedioxy-methamphetamine or Extasy), THC (tetrahydrocannabinol or marijuana), Heroin, and still cocaine. An alert security team is more likely to catch the seller than the individual users. I would look for someone that comes in regularly, alone, talks to girls but does not dance or socialize, and makes frequent bathroom trips. Your floor patrol and doormen probably already know who he is. Make sure your guys are not involved, because it is quite easy and lucrative to help out these guys.

Bathrooms are a common place for small transactions, but frankly it is often done in plain sight. Police no longer do the undercover operations, or even arrest drug sellers like they did in the old days. You may all know that prosecutions are down for several reasons—both practical and political. In fact, if the police do not care, why should we? People make their own decisions, right? Well, not so true. These drugs increase, and change, the effects of alcohol, resulting in either erratic and irrational behavior, or subdued, euphoria that ends in unconsciousness or close to it.

The result of that influence is accidents, of course—which we reviewed earlier. But worse are the bad decisions women make to become victims and the primitive brain impulses that cause men to become predators. This is hard to detect and prevent as well. Too often, I have had police come by the following day investigating a sexual assault where the last thing the woman remembers is being at the club. Not much to go on.

Your best options for prevention are to change the environment, educate the victim, or eliminate the suspect. (Remember the crime triangle?)

Environment—have you ever been to a place that had a full-time attendant in the restroom? That is not customer service, that is security. It is almost impossible to have sex with a bathroom attendant present. Drug transactions and consumption are equally difficult. And the bathroom does not get trashed either. Most clubs cannot afford to post someone in each restroom. I do recommend posting security near the bathroom to deter certain activities. This is just one layer of our multi-layered approach. See Posts. Otherwise, try to eliminate dark corners, poorly lighted areas, and blind spots.

Suspects—I am referring to drug suppliers and predators, who are not always the same person. I will talk more about this in the prostitution and trafficking section, but here we discuss club drugs. It is important to keep these guys out. Unless you catch them in the act, which is difficult, you will likely only know of them from tips. Some employees know and most patrons know who they are. Try to get that information. Then you can call the police, but your first priority is to get them out. See trespassing in Chapter 5, but basically kick them out and tell them not to come back. Remember that on private property we do not need to prove a crime; our suspicions are good enough reason. In fact, we do not need a reason as long as we are not discriminating.

Victims—we cannot exactly eliminate all our lady customers, but we can help educate them. Remind them to hold on to their purse and protect their drink. Bouncers will notice the ones that came in alone and can make sure no one preys on them. (Not saying to be a helicopter, just keep an eye on your guests.) At closing, and before, watch who leaves with that lone female. This is where it happens, whether from a date rape drug, or something she consumed willingly. Stepping in, even subtly might prevent a horrible night for her.

Date Drugs

Rohypnol is still alive and well in clubs. Also known as Roofies, it is the most infamous of the Mickeys in our modern age. It is a powerful depressant or sleeping pill, ten times as strong as Valium, that is no longer prescribed in the US. It is available from other countries without much hassle. Rohypnol was originally abused by cocaine and meth users as an antidote for the high. Date rapists like it because it dissolves easily, and besides drowsiness, wipes out the memory of the victim. My experience with victims is after two drinks (that they thought were normal) they pass out and their friends are surprised because she only had two drinks. Bartenders are often blamed for drink tampering.

It does not really make sense for a bartender to drug someone, but it could happen, and they do get accused. Like every other policy and surveillance method we employ, it is just as much to eliminate them as suspects as to catch them. So make sure you have the ability to watch your bartenders. Those cameras will also be useful to possibly catch the suspect.

As for suspects, I think they are like arsonists in that they like to watch their work. If you get a complaint, watch for the guy who is watching for the effects of his work. The normal things like removing abandoned drinks, making sure ladies do not leave them abandoned, and alert bouncers are good prevention techniques. I had one female bartender, when if she thought a bad guy was lurking, would offer lids to her patrons' glasses and she would also warn them to watch their drinks. What great service!

VIOLENCE

If you are having fights in your club, you may be doing something wrong. Fights are not caused by alcohol. Alcohol is just the fuel. Many studies have been done on the connection among bars, alcohol, music, and fights. They draw the same conclusion as anyone who has worked clubs for any amount of time. A grievance is generally the cause of violence in a bar. Makes sense, right? A grievance can be anything from a stranger flirting with my girlfriend, to stealing my table, to someone who bumps you on the dance floor. It is our job to observe these grievances before or as they happen and intercede before violence escalates.

We already have a dress code that we use to eliminate provocative clothing that will instigate a grievance among gangs, for example.

We need some environmental help as well. Whenever people are crowded, they are likely to bump and stumble. Not always a problem but it only takes one. As much as you can, alleviate choke points such as bathroom hallways and spaces between tables where people get funneled into a space too small to traverse without bumping.

Occupancy can play a factor just like chokepoints can. Therefore, we keep constant head counts. See the section on occupancy for more.

Visibility is a key factor in preventing fights. The mere presence of an authority figure may be enough to discourage someone. Deployment starts to become significant to the operation. You want to have security posted in such a way that they are visible to patrons, visible to each other, and have the entire place covered. More on deployment coming up.

Pre-violence

I am not a psychologist, but I did start using this concept called pre-violent behavior. We all know what violent behavior is: punching, kicking, etc. Pre-violent behaviors are those indicators that mean someone is preparing to fight. It may not only be aggressive behaviors, but also defensive and even provocative ones. I believe most of us recognize these behaviors but are hesitant to react until they become offensive. If your bouncers have this ability to spot these signs, you will not have any punches thrown unless you are under-staffed, or your bouncers are distracted.

We need to train our security personnel to watch for different things when they are inside a club. What we tend to do is look at girls (or boys), interesting clothing, strange noises, the band or DJ, and our phone. (!) We need to watch body language, for one. What do fighters do before they strike? Fists balled up, take their shirt off, square off—or take a fighting stance, signal to their buddies, and many more. These should be known to your people and is a great discussion (tabletop exercise) to have.

Taking Action

At the very first sign of one of these behaviors, get a backup and get in there. Use that charm and good looks to distract and separate. Remember the square off was started by some grievance. Took my chair, bumped into me by the bathroom, looked at my girl, embarrassed me, etc. If you can resolve this grievance simply, go for it. Be advised that getting someone a new chair does not resolve the conflict. That was just their excuse, in many cases. So use your discretion: You can resolve it and back off and watch or you can say time to go. Now ejecting somebody is a skill and can also cause a fight with you in the middle.

Ejections

Ejections should be hands-free unless an arrest is involved. We use force only in self-defense, not to kick someone out. Ninety-nine percent of your ejections should be verbal, touchless, and smooth. I have seen many different styles of doing this without anyone getting hurt. One is to be firm and friendly and ask the gentleman to step aside to discuss the matter while separating him from the other party and taking him toward the exit. If you can get him outside, invite him back tomorrow if you like but explain that is all for tonight. Take the other party out another way.

Other methods are what I call the swarm. Overwhelming them with numbers is very effective. It also gives an impression to your other guests that you are effective and unyielding. The bad side is, it is a distraction from the party and may look a bit too much. This why I say there are different techniques. A good bouncer can get most obnoxious persons out and down the road with a handshake goodbye. That is a good night.

Harder to teach in a book, I suggest role-playing with your staff and critiquing their real interactions.

Occupancy

Yes, believe it or not, occupancy is a factor in fights. Occupancy is determined by the fire department using a formula with multiple variables such as type of assembly, square feet, tables, exit size, and location. Of course, you want to get as many people in there as you can, but if you over crowd it may not be worth it.

More importantly, occupancy is about evacuations. When a fire alarm goes off, or shots are fired, occupancy will be the most important thing. Funneling 200 people through a 40-inch door and stairwell is just not going to work. The door host should have a clicker to count heads as they enter, subtracting those that leave to document hourly headcounts. One Fire Marshall I know does not count. He says if he can walk from one side of the room to the other without getting bumped, it is a good crowd.

Staffing Ratios

The question I get all the time from everyone is, "What is the right number of security to guests." The ones ignorant enough to give an answer to that will say anywhere from 1:50 to 1:125. These are truly arbitrary numbers because there are so many variables involved in this equation. I will go over each one with you.

Go back to Chapter 1 and look at Risk Assessment. You do not have to spend hours and hours or thousands of dollars. You may be able to do this on a napkin at the bar. Well, maybe a few napkins.

Determine the threats facing your bar or club: Weather, terrorism, and all those things, but especially fires and active shooters. How many people would you need to evacuate your occupants safely in either situation. I would do some research on the Chicago E2 evacuation and the Rhode Island Station fire.

Next, consider the programing of your venue. Is it a cowboy bar? Hip Hop? Square dancing? Will it have events like wet t-shirts, open mic night, ladies' night? How late is it open compared to your competitors? What was the bar before? How many officers did they have? Was it enough? What is max occupancy and expectations for reaching it?

Speaking of competitors: If you are new, go talk to them. Ask questions about numbers, problems, violence, etc.

Reach out to the police. They may have a liaison for clubs, but if not, speak to someone on swing shift or late nights. Ask them what type of incidents at this location or similar locations.

Now you have an idea of what your team will face. Look at your footprint. Restroom location? Smoking area? Number of exits? Emergency exits? Number of entries? Expecting lines? Dance floor? Separate rooms?

Here are areas and things that must be covered. Now if you are a small place, of course some will be covered by one person. Let's look at these areas individually.

Restrooms

Someone has to watch the restrooms. The restrooms are where much of the bad things happen. Women, especially find comfort in there because they can get away from men, noise, cameras, and leering eyes. Drugs are sold and used in there, sex gets it on in there, and sickness, injuries, accidents, assaults, and everything else goes down in there. Security needs to be there preventing, reacting, and resolving these issues.

Emergency Exits

Those exits better be wide and clear. People do not just evacuate for fires. Loud bangs, fights, strange smells, alarms, and numerous other events can cause people to run out. Your kitchen folks tend to use that extra space to store excess goods like cases of water, bags of rice, high chairs for the tables and even stacked tables and chairs from the dance floor. I cannot stress how important it is to keep this area absolutely clear. If you think you can store stuff away from the door, do the geometry. Imagine the triangle from the open area down to the 40-inch hallway that leads to that door. How are 100 people, screaming and shoving going to go from a 100-foot wide area to three feet? Even when calm, it is tedious. Now imagine there is a box taking up 18 inches of that 40-inch space. Then go look at the Chicago E2 Evacuation. It was not even a deadly threat or a fire, yet 21 people died trying to escape nothing. Your officer posted here will keep the area clear, even of loiterers looking for quiet space while also making sure nobody uses the exit. Under normal business conditions, we do not want the emergency exits used by patrons. The alley or parking lot or stairwell adjacent to the exit is not monitored well so do not send people out there. How easy would it be for a sexual assault, or some other attack to occur beyond that door without your knowledge. The alarms will help, but do not stop people from using them. You are likely not to hear it anyway. Plus, I know how to defeat them, do you?

Smoking Areas—These are a pain in the butt. You need it to keep your smokers from leaving, but the area produces no revenue. Since smoking areas are also a way in and out of the club, it needs to be watched just like an emergency exit. If you can do it, try to create a smoking area that is secure (such as a chain link cage). You cannot use the exit stairwell, even though everyone does. It will be worth spending a little money on a wall or something because you will save it on labor.

Other areas requiring coverage are covered under "Posts."

Re-entry

Letting people in and out of your club is an unnecessary risk, in my opinion. There are few legitimate reasons why people need to leave your club and come back in, avoiding the line. Unless your bathroom is outside, most trips are to the car to get the liquor they stashed to supplement those $8 drinks. Worse yet, are the ones who go out to the parking lot to use or buy drugs. Finally, there are hoppers that will go to your club at the beginning of the night when there is no line, get their hand stamped and return later to avoid the line at peak hours. This is making no money and takes up your time and labor. Heaven forbid there is a grievance inside, and one guest goes to his car to get his gun. It is surprising how having no re-entry improves security and reduces risk.

The re-entry needs to have the same search rules as the main entry. For the reasons I stated above, people will use it to circumvent your security. Dress code, intoxication level, attitude and ID all have to be scrutinized again just as they were at the main entry. You will need a hand stamp or wrist band or something and they are not tamper-proof.

Hand Stamps

There is no fool proof way to mark patrons for re-entry that I have seen. Kids, who are younger and smarter than me, can reproduce wrist bands, manipulate their removal, and reattach them on someone else. Hand stamps are smudged, washed off, and transferred via contact. Spend a little more money and get multiple hand stamp designs that are different each day. I have also used ultraviolet reflective ink that requires a UV light to be visible. These probably are the best but are still not 100%.

As usual, I will remind you of the risk of compromising security at this post. Take one of my examples of someone leaving and coming back in with a gun. You checked him at the main entry, but now he is back, and it is so busy you just checked his stamp and let him in. Anything he does with that gun is now the fault of you and the company. Even a simple ID switch at that post could result in a minor coming in, getting drunk, and crashing the car on the way home or going home with the wrong guy. Do not compromise your procedures at any of your posts.

ID Scanners

ID Scanners do much of the work of the door host. They can photograph each patron and their ID. This is useful for investigations when you need to identify a suspect from video. The facial recognition within can identify persons who have shared the same ID or who have been banned. If tied into a cloud and other venues, you can see people who were banned from another bar—and why. Scanners will do the math on the DOB for you and verify that the barcode or stripe on the back of the ID matches what is on the front. A bonus, which may help you get funding, is that it keeps a database of names and addresses your marketing people can use for advertising. The demographics are useful to see how many locals, how many women, how many over age 40, etc.

By the time this book is published I expect that the scanner will compare the ID photo with the photo you take of the guest. The technology exists but is a bit cost-prohibitive for most clubs. Except for that, the scanner you will have will require you to do that comparison yourself. The old trick of trading IDs is still possible unless you have an alert door host.

Closing Duties

Some venues kind of putter out in the last hour or two, and some go full blast up until the bell rings. Your deployment should be adjusted accordingly. Do not release officers unless capacity changes. Just because you close the entry does not mean those guys go home. Use them to watch the exit while the others maintain their posts until everyone leaves. Duties associated with closing are:

Mass Exodus—guide the crowd the way you want them to go. Do not send them out the back unless you have security there.

Post the entry hosts at the exit. Watch for drinks leaving the club; intoxicated persons who do not have a ride; the lone female I mentioned earlier who may be headed out with a stranger.

Depending on your location, patrol the parking lot. Prohibit loiterers—loitering leads to fights; make sure nobody gets in car intoxicated; keep watching for those loners who may be taken advantage of.

When club is clear, do the safety sweep. Look for abandoned property, drugs and paraphernalia, weapons, suspicious items. Final check of emergency exits.

Escort employees to their cars.

Many employees will stay after work for a drink or two or three. This is risky business, but I understand it. If your employees do it, then make sure someone is responsible and ensure everyone gets home safely.

POSTS

We are going to go over each security post in a club. This must be scalable depending on the size, exits, volume, and all that; so do not think that your little corner bar will require 14 persons to fill all the posts. Some people will cover more than one post in a small place and sometimes you will need more than one at some posts in a crowded place.

Line Control

If you are fortunate enough to have a line to get into your club, you need to supervise it. Lines take on a life of their own if not properly guided and watched. Stanchions or some other type of guidance is necessary even if it is a straight line down the sidewalk. In fact, many municipalities require you to have certain controls on your line, cannot block the public right-of-way and all that. A line of about 30 or more people will need a security officer to attend to it. This is good, because he/she can do a lot of the door host's work for him before the guest gets to the front.

Back to the queue. Do not wrap a queue line unless your space is limited. The more people are crowded together and are face to face, the worse their behavior is likely to be (at least with younger patrons). If your line is outside, as on a sidewalk, make sure you are following city ordinances and being a good neighbor. Consider having trash cans every few meters. Though these are not your guests—yet—they are there to be your guest and they are under your control, so to speak, so make sure there are no hazards or ways to get injured.

Behavior in the line is a perfect way to foresee the future. If someone is hassling girls, or cussing, or being a jerk, that is how they will be in your club. You need to refuse service to him/her. Warnings do not work because if he is going to act up right in front of you, what good is a warning? Besides, what if you allow him entry and he assaults someone inside? I would say it was negligent of you to let him in when you knew his behavior was not acceptable.

Dress code violators will stick out like a sore thumb in line. Save them and yourself some time. Maybe they will even have time to go change. It is pretty bad to have someone waiting in line only to get to the front and find out they are not acceptable while you were watching them the entire time. Place your dress code sign at the front and the end of the line for the same reason.

This is a good time to weed out the intoxicated ones and of course the minors. The door host will do a thorough check, but you can ask minors how old they are. Then it is on them if they wait in line and get turned away. Those with drinks must go. If you are on the sidewalk, it is illegal to have a drink anyway. Intoxicated persons need to leave, and they will not like it so get backup if you can and be careful. Remember to make sure they are not driving. Offer a taxi or some other means home.

Rowdy Behavior—Persons who engage in horseplay in line are going to be even a bigger problem when they consume alcohol and let go of their inhibitions. The promise of "I will behave" is not likely to be kept and puts us at a disadvantage.

Prohibited Items—Though this will be handled at the door, the line officer can ensure compliance and save the guest an unnecessary wait by advising them of the rules on prohibited items.

Pre-Violent Indicators—Patrons who exhibit those behaviors that we know to be indicators of violence require some scrutiny before being allowed entry. We use the short interview to do this discreetly without escalation. (See Violence later in this document.)

A good, orderly line will get you in good favor with police, city officials, and the neighbors. They can make your life—and your line—miserable if they want.

Door Host

The door host (and there may be more than one depending on volume) is the key to the operation and may often be the lead officer. The door host is the "face of the club" as he/she may be the first person, and the first interaction, that each guest will have with our staff. This interaction sets the tone for future behavior and determines the atmosphere of the venue.

Post Setup—The Door Host will set up the entry post at the beginning of the shift. Stanchions, worktables, scanners, and other items must be set up according to guidelines ensuring a safe stand-off from the door, a choke point to funnel visitors single file, and with enough space for safe egress and guest encounters.

Greeting—The greeting is key to meeting guest service standards, setting the mood, and evaluating attitude, behavior, and intoxication level. Each host will make eye contact and offer a verbal "welcome" or other greeting as the first step to behavioral recognition. I suppose some instructors might tell you that the "Tough Guy" approach needs to be used at the first encounter. Some feel that playing the role of the alpha male, complete with a stare down, will establish dominance that will be used later to control the guest. I think that might be good in prison, but this is a nightclub and people are here because they want to have a good time. I also think the opposite method is better anyway. Use those guest service skills, look the person in the eye and offer them a sincere welcome (just like they walked into your house). Be friendly with our guests and they will be friendly with you.

Behavioral Recognition—When you say welcome to someone, and you do not get the response you expected, there may be a reason. Continue to ask questions: What brings you here? Celebrating something? Been here before? Etc. If you detect "attitude" this is a form of pre-violent behavior and needs to be eliminated or adjusted. Pass him off to your second for more scrutiny. If he gives you attitude for no reason, then what is he going to do if someone spills a drink on him?

If, on the other hand, you detect alcohol, engage in a little more conversation until you are sure. Nothing wrong with having a drink prior to arrival, but any level of intoxication and it's going to be downhill for us inside.

ID Verification—Though there may or may not be a scanner or other tool to assist the host in verifying identification, the responsibilities are the same. An ID must be Valid, genuine, belong to the guest, and prove that the bearer of the ID is 21 or over. The host also must watch for those who pass IDs back to their friends. (See the section on ID Requirements.)

Violent Indicators—Besides the attitude mentioned above, any type of physical violence is an absolute No Way. Same reason as above.

Headcount—The door host will maintain a log that indicates the hourly occupancy of the venue. This is done using a hand-counting device ("clicker"). The door host should know the number of bodies, including employees, at all times and be prepared to suspend entry if count reaches maximum occupancy. Remember to account for those leaving.

Log—The log does not have to be at the front, as long as you have one. Keep the headcounts there by hour. Log any activity—mentioned throughout this section—such as ejections, fights, complaints, VIPs, etc. This makes it so much easier to follow up a week later if someone comes forward with a beef.

Dress Code—The door host also enforces the dress code. Have a procedure in advance for exceptions or complaints. Decide who can override or deal with stubborn patrons. I always feel some satisfaction when someone does not meet the dress code and they go into a rage, cussing and threatening. I feel like, "Yep, it works."

Exit/Re-entry—Try to locate the exit near the entrance to allow the door host to easily count the occupancy. It also makes better use of staff. The door host assigned to re-entry will be responsible for applying hand stamps, controlling VIP entry if any, and ensure persons leaving are doing so safely.

Floor Person

Floor persons are those who work inside the venue and may be posted or roaming depending on staffing levels and the size of the room. The floor officer is responsible for carrying information to and from the door host, keeping the room safe, and initiating contact with guests.

1. Secondary Exits—Generally, clubs have a main exit at the front (near the entry) and emergency exits on the sides and/or rear. Officers may be assigned to one of these secondary exits to make sure they are kept clear, that no one uses them for unauthorized exit/entry, and to ensure that in an emergency our guests and employees can find their way to the closest exit.
2. Dance Floor—Each venue will generally have a dance floor or open space designated as such by management. The officer(s) assigned here are roamers who keep this area safe by: watching for pre-violent and violent behavior; alerting other officers to problems; keeping prohibited items off the dance floor (drinks); and attending to wet spills and other safety hazards. In smaller venues, the dance floor officer will also ensure that no one approaches the band or DJ.
3. Restrooms—One officer may be assigned to the restroom entrance to watch for: loitering, drug use (and other criminal activities) cross-gender entries, and indications of violence. This patrol includes regular walk-through of the appropriate gender restroom and ensuring the other gender is patrolled by another employee.
4. Contract Security—Some clubs will hire a guard company to supplement their bouncers, especially for special events and holidays. I recommend giving these officers simpler, less risky duties. Work these "post orders" out in advance so there is no confusion. Effective uses for these extra bodies are:

   Watching emergency exits
   Watching restrooms
   Safety sweeps
   Crowd control—providing directions
   Parking Lot Patrol—if they are trained and contracted for that purpose

Contract officers should not be assigned to:

Checking IDs or serving alcohol. They do not have the training. This is your alcohol license on the line.

Confront guest behavior—Not trained. Do not know our policies.

Respond to fights, eject guests, make arrests, anything physical. Not trained and this is too risky and a huge liability. Of course if someone is getting their butt kicked, that is an emergency and they should do what they can that is reasonable—even if it is, alert others.

Make sure your contract covers liability for their actions.

SITUATIONS AND PROCEDURES

Lead with accidents. Slips and falls are common where there is food and beverage, and they are often the fault of the facility. They are costly to the guest in pain, time, and medical bills. It is also costly to you for the same reasons, sort of. A guest who has an accident in your place may want to hold the place responsible. Your patrons have an expectation that your facility is safe and that they can enjoy themselves without worrying if there is a lose handrail, a puddle of water on the floor, or a chip in their glass.

It is management's obligation to prevent safety issues before they cause an accident. This is not difficult, but sometimes we get distracted by a million other things. If the company is going to pay for a $50,000 broken hip on a night where the revenue was $5,000, you can see how our priorities may be upside down. Safety is always the right thing to do anyway. The way to make sure you do not miss something is to create a process.

1. Safety sweep—At the beginning of each day, assign someone or a team to check the entire room for safety hazards. Spilled liquids, loose chairs, lights out, and whatever else you have. Check the seat cushions, under tables, and other hiding places. You are likely to find pills, bottles, syringes, and all sorts of things. Start fresh and clean.
2. During the night, assign someone or ones to monitor the floor for spills. Depending how busy you are, this may be a full-time job. Our team would place towels in strategic locations so a spill could be easily mopped up in a second or two. The dance floor is a good place for this.
3. Assign someone to patrol around the venue to pick up abandoned and empty glasses and bottles. This prevents spills, weapons for fights, and tampering with someone's drink. Watch for patrons who remove their shoes. This should be a policy because there may be broken glass or someone stomping on them.
4. Restrooms are a major hub of all things (and have their own section coming up) but keep them clean. Floors are normally wet in a restroom, but that does not relieve you of responsibility. Wet Floor signs may help, but if you have a particularly messy clientele, you may need a mop handy in there. Then there is tissue paper, vomit, and whatever else to fall on and in. Nobody wants that so keep it clean.
5. Back of the House—The kitchen or back bar or scullery is just as important. If you are not using rubber mats and requiring kitchen shoes, you are asking for accidents. Protect your workers. You do not want anyone to get hurt on duty and, besides that, being down a bartender or server on a busy night will affect everyone else as well.
6. When I recommend assigning someone to these tasks, I am not trying to increase your payroll. Some employees will have more than one assignment. All employees should be aware of safety hazards, however.

A beverage server is carrying a tray full of drinks across a crowded floor. Someone bumbles her, the tray jostles, and some of the drinks splash over the side. Otherwise she is intact and moves on. She looks down as she walks to her table and sees some liquid on the floor, but she cannot get down there in this crowd with a tray, so the shoulders shrug and she goes to get her tip. Handsome Bob walks through the puddle and slips and falls, twisting his ankle. He is helped up by security, the spill is cleaned, and he says he is fine and will walk it off. A friendly female tells him that the server accidentally spilled some drinks. "It was not the server's fault but would have been nice if she cleaned her mess."

The next day, he wakes up and his ankle is swollen, and he cannot even put on his shoes. Bob is an actor at the local community theater and now he will not be able to shine as the Duke of York in the little theater's rendition of Hamlet. Bob has no insurance, being a struggling actor, so he contacts the bar owner and asks for some assistance with his medical bills. The owner (or risk manager, if you have one) says the bar did everything they were supposed to, security responded right away, cleaned it up, offered him assistance, offered to document the incident but he said he was Ok. Seems like they did everything reasonable. Bob explains that the spill was from his server who ignored it, and the owner says, not to my knowledge. Sorry buddy. How about a free bottle next Saturday?

A week later, the bar owner receives a letter from an attorney, demanding that he save all relevant video and his insurance information. This just escalated from about $1,000 to about $25,000. It is going to be costly to defend whether you are right or wrong. The facts are not in your favor because your server ignored a hazard that she caused, you did not get a statement from the witness, or the patron who fell, and you did not document the incident. Worst of all, the video has been looped over and it's gone.

Solution: when there is a spill, no matter who caused it, the employee needs to stand next to it, warn patrons and wave her arms wildly until another employee brings the towels. Leaving that spill to go get towels will cost you. Next, document every accident, no matter how minor. You do not necessarily have to write a full-blown report, but at least get the information for guest, witnesses, and employee. Then, make sure you pull video as soon as you know it is serious. When he called the owner is when wheels should have started turning.

Violence

If you feel that Violence was already discussed in this chapter, you are correct. My intent in the first part was to explain the impact of violence and fights on the operation and generally how to deal with it. Here, I make it one of the situations to which our staff will have to respond. So some of it is repetitive but is worth reviewing.

Pre-violent indicators—Experienced security officers can stop a fight before it starts. It is imperative that door hosts address these situations before they get out of control. The following behaviors will prompt an officer to take a second look and intervene if necessary.

Arguments—A verbal disagreement in and of itself is not an indicator of violence. The officer must look at facial expressions, body language, and reactions from others nearby.

Yelling—Yelling in a noisy bar is normal and acceptable. Once again body language can give cues on what the person's intent is, if any.

Intoxication—Alcohol decreases a person's inhibitions and can lead to violence in a few ways. Drunks become clumsy and have little regard for persons around them so an accidental bump can lead to a violent reaction. Because of reduced inhibitions, a simple look can provoke an intoxicated person to violence. Overly intoxicated persons should not be walking around "looking for a fight" anyway. Put them with friends to go home.

Body language—"Squaring off," puffing chests, removing shirt(s), even a frown or a grimace can mean a fight is about to occur. No need to wait. Get in there with a backup and ask questions. This behavior may be reason enough to escort the person out.

Ejections

An ejection is removal of a person who is exhibiting pre-violent behavior or intoxication. They do not need to be trespassed necessarily because we are hopefully preventing a problem, not reacting to one. A person who is being ejected simply needs to be asked to leave. Rational persons who will be welcomed back will cooperate and leave. Someone who refuses needs to be trespassed.

Intoxicated Persons

The "cut-off" is a detrimental attempt at salvaging a patron and it is rarely effective. While he/she is in the bar, they will find a way to have another. Do not "cut-off" intoxicated persons and allow them to stay. If they are too drunk to drink, they need to go home safely. Grossly intoxicated persons should not be allowed to remain as they can become unsuspecting victims, provocative suspects, and a drain on resources. Accompany them to the exit. At the exit, one of the following should occur:

- Allow his/her companions who are relatively sober see that he gets to his next destination safely.
- If no one is available or capable of caring for our intoxicated guest, he/she belongs to you until you find safe passage for them: A willing taxi, a ride share, and the police if necessary. Not the guy standing on the corner smoking a cigarette. Treat her like she is your sister or brother.
- Extra care should be taken that a female is not left in the care of males who may have bad intentions. When in doubt, have security accompany them to a safe location.

Trespasses

Trespass is our best tool to prevent violent, criminal, or unwanted behavior. Persons who are violent or otherwise disrupt our business should be trespassed. You will have arguments with management to the contrary. They will ask you for a cooling off period or come back tomorrow. In my opinion, if you allow someone to come back that exhibited violence already, then it's going to be your fault next time. This is the definition of foreseeability mentioned throughout this book. In chapter 5, whatever the owner wants—it is his bar. Trespassing procedures are located at XXX.

USE OF FORCE

This is where everyone gets in trouble and it does not have to be complicated or misunderstood. The problems usually arise from lack of a policy, lack of enforcement of the policy, or insufficient training on the policy. I am going to resolve all three of those issues for you, so you can run a safe operation with no injuries and hopefully no complaints.

Policy

Before we get into the policy, I urge you to reconsider your past policies, police departments or the military because civilian security is much different and subject to different laws and standards. Most police departments still use the "Use of Force Continuum" or Ladder of escalating force, despite the fact that juries do not understand them. In fact, no one understands them, as we have seen from numerous riots that started from a police officer shooting someone with a knife or "taking" someone who was empty-handed. The question by activists is always "why didn't you use a less-than-lethal weapon." I am not an expert in police use of force, but I am for security, having worked both sides of many cases involving excessive force. If the program I lay out for you here is followed, you really cannot have any problems. Oh, you will have fights and some injuries, but none that are your fault.

I used to use the "continuum" or "ladder" because we had guns, Tasers, pepper spray, and all the tools. It worked pretty well until we found one of our officers in a deposition trying to explain when you use which level of force. While a police officer has months of training and much more practice, we have a huge turnover and a fraction of the training. So, we made it simpler.

I had a brilliant training manager who researched this stuff extensively and practiced and trained it as well. He found that some police departments were changing their policy to simply say, use that level of force necessary to overcome the threat presented. One example he gave was a high school girl pulled over for speeding. She refused to roll down her window for the police. Using their "continuum," they escalated through each level, finally breaking the window, and using the taser to get control of her.

Imagine that "power" in the hands of a security officer. We would be getting sued and injuring people all day long. So, using a similar scenario, suppose the same girl is in your club, refusing to leave. Tackle her to the ground with four guys and handcuff her, right? What was the threat again? Oh, there was none. The arrest is legal, I suppose but what if you injure her in the process? We have other resources like calling someone to talk to her, calling the police, bribing her with a milkshake, whatever. We have all day.

Here is an example of a real policy that has been used and "court-tested." Remember this is only part of the solution.

The policy explained below applies to Nightlife Security employed by Company X. Officers may not use physical restraints or carry and use handcuffs without the associated training. No level of force may be used without the associated training approved and sponsored by the company.

PURPOSE: Situations may arise where it is necessary for security to use various levels of force to protect themselves or others from imminent physical harm. As always, if you do not fully understand any portion of this policy (or any others) you need to speak with a member of management until your questions are fully answered and you feel comfortable with your understanding.

Use of Deadly Force—Security personnel, in accordance with federal, and state laws, are authorized to use deadly force to protect the officer, or others, from what is objectively and reasonably believed to be an imminent threat of death or serious bodily harm.

Use of Non-Deadly Force—In all other use of force situations security personnel may use only that level of force that is objectively reasonable to bring an individual under control.

NOTE: Regardless of the level of force used, or the force being employed, all force MUST STOP as soon as the subject's resistance or attack ends, and the subject has been taken into custody where applicable. Also, officers are not permitted to use their body weight on a subject's head, neck, or upper chest, for the purpose of restraining combative subjects.

Excessive Force: The improper use of force occurs when the type or degree of force employed was unreasonable. The use of improper force will not be tolerated.

For those of you who saw "Deadly Force" and gasped out loud, take a deep breath. I am not talking about arming bouncers. Deadly force can happen with bare hands, and sometimes does, whether we like it or not. If you do not have a policy to enforce, how will you keep your people from being excessive? This clause is here so the officer can protect himself or someone else from death (or serious bodily injury). For example, if he is being strangled, he is authorized to punch the assailant in the face over and over until he stops, or break his neck if necessary.

I do not expect you to deploy any weapons, but if you do, you need to have extensive training and scenarios explaining when they can be used.

Many owners and insurance companies want a "hands off" policy. This is not practical in a nightclub or bar. The policy above is hands off unless officer is defending himself or someone else. Yes, we are going to go hands-on all night long, but we need to train when it is acceptable and when it is not.

This policy needs to be enforced. I can tell you from prior cases, that when an officer kneels on someone's neck, it generally gets ignored as long as nobody was injured. Now three months later he does it again and kills the combatant. Then I find that you had a prior incident that was not disciplined or re-trained. Now guess what?

You don't have to fire someone for a mistake, but you do need to make sure it does not happen again. That means document and re-train.

Officers, well, anyone, that is not effectively trained will revert to past experiences or training. So, you hired a rough and tumble Roadhouse bouncer. It will take more training to re-teach him than the guy who was a bartender. Our training should consist a little bit of policy and law (classroom) and majority of practical application. Get someone certified to teach these maneuvers. If you have a police officer or martial artist do your training, make sure they understand that we employ defensive tactics only. No stop and frisks, detentions, come-a-longs, etc.

EMERGENCY PROCEDURES

Person Down

Accidents—As I mentioned before, this is the most common claim in a bar or nightclub. Accidents will happen, and you will not prevent every one. It is generally how you respond that puts you in better graces with your guest. Following these procedures are more likely to protect your establishment.

Of course, medical attention (guest safety is always first). If conscious, ask if they want an ambulance. If you suspect it is worse than the patron thinks, call the ambulance anyway. There is no charge for this (in most cities) and the guest can refuse service from them. If there is a head injury, call the ambulance anyway. If guest is unconscious or was unconscious or is disoriented at all, call the ambulance. Never diagnose or talk the guest out of treatment.

Do not accept blame or offer any excuses. Just get the facts and the guest's side of the story. Avoid statements like "That is always a slippery area" or "that is our third cracked glass tonight."

Document the incident, take photos, and pull video (not for the patron, for your investigation).

Write down statements made by the guest, even if they do not want to write anything. Get witness names and numbers.

If there is an immediate hazard like a spilled drink, photograph it and clean it up.

Accidents should always be investigated, interview witnesses, look at video, examine photos so you can defend the claim and take steps to prevent it from happening again. Not doing this can make you look negligent. More detailed steps are included in the Investigations Chapter.

Illness—Follow the same protocol as for accidents. When in doubt call an ambulance. An investigation on an illness is not necessary unless you think the bar has some responsibility (food poisoning, intoxication). At a minimum, obtain names and numbers in case someone comes back investigating the episode.

Remember in any situation, do not allow employees to do first aid or treatment unless those skills have been trained by your company. They represent the company and anything they do will be your responsibility. For the same reason, do not diagnose. Refer everything to a qualified medical person.

Fight (Two or More Persons)

This is a difficult situation, not only physically, but legally. Preventing and avoiding fights is always best.

A bar that has fights on a regular basis is not acceptable. It means you are doing something wrong, whether it is your personnel, training, dress code, or any of the other things discussed in this chapter. If someone gets hurt at one of your many similar fights, eyes will be on you and your policies as to why you knew you had a problem and did not remedy it. I will explain how to remedy it at the end of this section.

Let's break down the elements of the fight and prioritize our response.

While fights involve two parties, they are rarely limited to two persons. Each combatant will have friends and bystanders who want to help. This is generally in the form of more fighting as opposed to pulling back their friend. A security officer approaching a fight, which by definition is two or more persons, is outnumbered. One officer getting in the middle of a fray is not only going to get injured, but more resources will be needed to intervene.

You are not going to be able to read here how to deal with a fight. Everyone has their own technique, which depends on physical ability, cunning, number of combatants, number of good guys, the surroundings, and the bystanders.

As you role play and practice this with your team, I recommend that you consider the following:

1. Make sure it is a fight. Three people on top of one guy is not a fight—it is an assault, or worse. You have a duty to stop that immediately.
2. Be reasonable in your actions. It is OK to use force to defend yourself as you attempt to stop the violence. It is not OK to use offensive gestures in the fight (Punching, kicking, throw downs, etc.).
3. Technique 1—Overwhelming force. If you have the staff, get in there, break it up, stop the violence, and get them out of there.
4. Technique 2—If staff is scant, go after one party. Take the "tougher," more aggressive one pull him back, safely and completely.
5. Technique 3—Go after the weaker one, pulling him back and "rescuing" him from the pummeling. (Remember the crime triangle—take away the victim, suspect, or location.)
6. While I mentioned earlier that we do not lay hands on someone unless it is defensive or part of a lawful arrest, this is the exception. Breaking up a fight is a "reasonable" reason to use "force." However, it is especially important that the force is reasonable and that the force stops as soon as the objective is achieved.
7. Training is vital. Do not wait until an actual fight to find out how your new bouncer reacts to a fight. I have seen many incidents where a new officer, even trained, does a sideways tackle on someone who was otherwise cooperative.
8. When the first officer gets there, he/she needs to take some action while awaiting backup. Standing there and watching gives the perception that we are not going to act, that we do not care, and that this happens all the time. "Loser goes to jail!" is not a good response.

In 2017, the Nevada Supreme Court reversed a lower court ruling that a fight near a casino nightclub was not foreseeable because it was not in the club as with the many other fights. The higher court said foreseeability was "a totality of the circumstances," apparently observing that a fight outside the club is close enough and related to the casino. In the opinion, the court observed that the lone responding officer waited "12 to 15 seconds" for backup to arrive before intervening. This called into question the "staffing and response times" (Humphries et al. v NYNY Casino).

We must weigh immediate action against officer safety based on the court ruling in the adjacent textbox. I recommend training the first lone officer to order combatants to stop and even order them to leave the premises. That may not work physically, but it may help you put a trespassing charge on them when you get them calmed down. Keeping bystanders away is another function they can perform while waiting.

Once the fight is over, now what? This tendency to separate the parties, pull out the notebooks and start asking what happened, are ridiculous in my opinion. Who cares what started it? We are not the police trying to develop a case based on statements from witnesses and victims. They have disrupted our business—get them out of there! Now if they damaged something and you want to see about getting your money back, go ahead, but it's not worth it. The entire club has stopped functioning to watch this fight. Nobody is dancing or buying drinks while security does their investigation. Get them out of there.

Sometimes one combatant will say he wants to press charges against the other for battery or assault. I would not get involved in that. Use your cell phone and call the police, I would tell them. If you start arresting people on someone's behalf, it is going to go bad, legally. If you want to make arrests and be more of a "zero tolerance," talk to your local police or city head of most frontline police officers so ask someone in command or the attorney that takes these cases.

If one is clearly a victim, you have an assault or robbery on your hands. That is completely different. Get a police report and document just as you would any incident. You may have to defend your security system from him down the road. Use that investigation to determine corrective measures, if any.

Ejecting combatants from a fight is straightforward. Except for the "victim" scenario above, everyone must go. Anyone that participated, whatsoever, has shown their poor decision-making ability and needs to go home. Take opposing parties out opposing doors. If you do not have a second exit, hold one party, or get them out and guide them opposite ways outside. Do not throw out someone that needs medical attention. Get them outside and call an ambulance. That will bring the police, in many cases, so be ready for that investigation.

Speaking of police, if you get sued for anything to do with an assault, the plaintiff will run a "calls for service" report with the police department. This report, depending on the agency, will provide dates, times, and details of every time the police came to the bar. It will be used to make your bar look like a violent, out-of-control, dangerous dive bar. In fact, I know several bar owners that avoid calling the police at all costs for that reason. This causes violence to escalate farther than necessary, go unchecked for too long, and makes your reputation and environment even worse in the long run. Having sat on both sides of those cases, I recommend you keep a daily log of events and whenever the police are called for anything. That way if you are ever defending your history win litigation, you can go down the list and say "this one was a fight on the sidewalk that we broke up," "this one was a female victim reporting a fight down the street," "this one was a report of shots fired that someone called in as a prank," etc.

Ejections

Ejections, bans, 86, trespasses—whatever you call it, it is the act of kicking someone out of your establishment for a time that you determine. Some of the reasons you eject someone are, creating a disturbance, pre-violent behavior, violent behavior, bothering patrons or employees, theft, and miscellaneous minor crimes. Contrary to the movies, ejections are done verbally and not forcibly. Did you know that technically, if you grab someone's collar or push them toward an exit, you are committing battery? If you forcibly move them from the bar to the exit, that is kidnaping (or some other legal term in your state that means the same).

Using force to move a person that does not want to be moved, is not only dangerous, but can bring in others to the conflict that will complicate things. You need to develop those personal skills that coax someone outside. Let them vent, tell them it's too loud in here, try the girlfriend or wingman, etc. You have plenty of time, but if he is not battering you, don't batter him. I always use the measure of what if it was me. Would I let some guard put his hands on me?

For someone who is stubborn, you have a couple of options. One, you can call the police. They can forcibly remove someone. Two, you can use the trespassing law. In most states, telling someone to leave, and their refusal, is a misdemeanor for which you can arrest them. The threat of this is often sufficient but you need to back up your threats with action. If this is a new method for you, talk to your police department first. In casinos, for example, we used to trespass all day long. It is a highly effective tool because there is really no defense or argument against it. Where you there? Yes. Did you refuse to leave? Yes, but…Sorry. Guilty. Trespassing does not need a reason (unless you are discriminating—and that is hard to prove).

There are a couple of instances where putting your hands on someone is OK. Obviously medical attention, like CPR is reasonable. If someone is having trouble balancing or walking, an escort-type grip on their arm is reasonable. The key word is "reasonable." People get everything on video. Would you want a video of you pushing someone out the door? Or worse? You cannot defend that. Breaking up the fight with force is reasonable. Document every physical contact you have.

The following procedures are outlined in the chapter entitled "Emergency Procedures." These are brief reminders for your procedures. Make sure you have a plan for each of these that you practice with your employees.

Much of the evacuation training and procedures are included in Crowd Manager training that I recommended before. I strongly recommend that online course.

Fire Alarm—Sirens and Strobes

1. The alarm should override the music. If not, inform the band or DJ to stop the music.
2. Advise the person in control of the sound system (if possible) to make announcements.
3. Most people will not evacuate when there is an alarm. Designate someone who will order the evacuation. Check your fire code to see if evacuation is required. Because most injuries occur during the evacuation, the fire code may allow for an investigation period when the alarm rings. That means evacuation is not required until smoke or fire is confirmed.
4. When in doubt, or when patrons want, evacuate.
5. If evacuation is warranted, direct guests to emergency exits in a calm manner.
6. If not evacuating, keep guests calm by providing updates until alarm is reset.
7. Alcohol service will be suspended during an alarm.
8. Direct evacuating guests and employees to a pre-determined location outside.

Smoke or Fire

1. Direct guests to emergency exits in a calm manner.
2. If exits are blocked by fire or are unsafe, use alternate exits.
3. There may or may not be the closest, safest route. Employees should be trained to guide people to the closest emergency exit.

Power Failure

1. We will not evacuate a venue unless instructed by the authorities. There is not much point to going outside unless the failure is prolonged.
2. You should have emergency lights on the walls and ceiling that come on when power goes out. They will last an hour or so.
3. Use flashlights to keep guests calm and allow those who want to leave, a clear exit.
4. Someone should inspect the building to make sure the failure was not caused by something like a fire.

Earthquake

Tremblers are usually over before anyone realizes or has time to react. Our concerns would arise in the wake of shocks and falling debris.

1. We will not evacuate a venue unless instructed by the authorities or a property= maintenance official who deems it unsafe.
2. Keep guests and employees calm and shelter-in-place.
3. It is safer inside than outside.

Hurricane/Blizzard/Tornado

1. Stop entertainment and use warning radio.

2. Shelter-in-place, using designated shelter, if possible.
3. Keep guests away from windows and exterior walls.
4. Kitchens and bathrooms are generally safer places.
5. Make sure this has been pre-determined.

Active Shooter/Shots Fired

1. Remember Run Hide Fight.
2. Assist guests with evacuating away from the shots.
3. Seek shelter if evacuation is not safe.
4. Call 911 with exact location of shooter.
5. Keep guests and employees from going into danger area.

Most buildings constructed after the 1970s are designed to withstand a moderate earthquake. Unreinforced masonry (brick) buildings—commonly seen on the east coast—are likely not safe in an earthquake. This was evident in the 2014 Napa Valley, CA earthquake. A 6.0 earthquake killed one and did an estimated 362 million to one billion dollars in damage. The buildings in Napa and parts of old California are brick and many collapsed during the 3:20 a.m. rattler. It was fortunate that it happened so early, and on a Sunday.

RESTAURANTS

Like every other part of a hospitality venue, guest safety is paramount. The hectic, fast-paced environment of food service provides many opportunities for accidents and careless behavior. Slip and falls, covered earlier in this chapter, are the most common accident.

Slips, Trips, and Falls

Usually spilled food or drink is the cause of an accident. Close attention needs to be paid to anything such as an unfortunate design flaw that needs to be addressed. Dining lighting is low and steps become invisible to an unfamiliar guest, who is focused more on winding past tables and chairs while looking at the décor than looking down at steps. If they cannot be removed, make sure steps are very well marked, lighted, and get a verbal warning each time a guest passes.

Restaurants want as many tables and chairs as possible to increase volume and the resulting revenue. This causes several problems. One is that the aisle ways become narrower and thus two persons cannot easily pass without bumping into each other or the chair of a third patron. Two, servers carrying trays of food are more likely to trip and dump their goods all over someone. Third, patrons will tend to push their chairs back into the aisle way. Speaking of chairs, if you have any influence in your restaurant, talk management out of using chairs with angled legs. These are a common trip hazard. Straight legged chairs are better.

Employees deserve some safety, too. Floors in a kitchen should be non-slip surface or mats used throughout. Walkways should be kept clean in all shifts. Cuts are common for kitchen workers so make sure they are using safety gloves, following proper techniques, and that machinery is maintained and has all of its safety guards.

Food Poisoning

Anytime someone gets a stomach ache after dinner, they are likely going to make a food poisoning complaint. I am not a physician but I do know that it takes some time for a bad meal to start showing symptoms, so it is hard to determine which meal or food caused the ailment. It is best to document the illness and let the risk manager deal with the guest.

Do not accuse a guest of faking or exaggerating. You will lose this argument. They will tell the doctor your chicken smelled and tasted funny, he will blame it on that, and you will be outnumbered. Instead, gather as much information as you can. What they ate, when they ate it, when symptoms started, etc. Then have the chef check his inventory just to make sure he did not have a bad batch of something. Finally, gather stats on how many of each item on the guest's list that was served that day: 72 hamburgers, 45 salads with ranch, and so forth. If the guest makes a serious claim, the risk manager can use the stats to show that x number of meals were served and only one guest got sick, so unlikely it was from us.

Likely most complainants are looking for a free meal. This is probably a cheaper route for the restaurant, but does not mean they will not still come back with a claim. Use discretion on that.

Allergies

If you have noticed just about every menu has disclaimers about allergens in the food. "This ingredient was carried past a room that had peanuts." But seriously, restaurants do this because of claims received from unknowing guests who did not realize that pistachio-encrusted salmon has nuts in it. The documentation procedures are the same as above, except an ingredient list will help the risk manager in this case.

Now the Financial Stuff

Walk-Out

The "dine and dash" is still alive and well. Teenagers and large groups are the common offenders (the servers know this profile well). My recommendations for dealing with walkouts are as follows:

Servers tend to know who is going to walk-out and they are the only ones that do. They should do whatever they can to head off persons leaving and attempt to recover their money.

If your restaurants have policies of charging walkouts to the server, eliminate it. This encourages your servers to chase people through your hotel and will make you responsible for injuries to either party.

I encountered a different violator that became common in our region. A homeless person would come in, sit down, and order a meal. When it was time to pay, they said they had no money, no way to get money, and have no problem going to jail. (Jails are overcrowded and process them through and out.) There is little to be done with these folks.

For the others, your best recourse is to stop them and negotiate payment. Call a friend or relative, try all the credit cards, see if they are a hotel guest, etc. I would not necessarily arrest someone for this crime unless they are a habitual offender, a child that needs to be turned over to an adult, or some other extraordinary circumstance. If you do arrest, mind the following:

- You will not necessarily recover the loss.
- Your server or manager who has to sign the complaint will be gung-ho until court date comes and then you are in a pickle.
- An arrest involves either walking a scruffy guy through your nice hotel in handcuffs, or having at least two uniformed police officers disrupt the scene at your restaurant.
- Defrauding an Innkeeper, which is the crime for walkouts in most states, requires proving “intent.” Intent is difficult to prove if someone said they forgot their wallet.

Better to arrange a payment.

Credit Cards

There are so many ways guests and employees rip you off in your restaurants; it is almost considered a price of doing business. Most of these crimes occur due to weak procedures or supervision.

First and foremost, follow the procedures laid out by your credit card companies. Following those procedures protects you from the loss. These include following minimums for obtaining ID, signatures, and prior authorizations.

A cashier separate from the server alleviates many scams perpetrated by dishonest servers. The more people involved, the less chance of collusion or lone-actor frauds.

Servers and cashiers can steal card numbers with the camera on their phone, with a scanner, or just by writing it down. Keep a surveillance camera on the POS terminal and check the video often if you do not watch it live. Prohibit phones and personal belongings from that area.

A cashier at a snack bar where there is no verifier can alter a receipt by filling out the tip line. Guests rarely notice a dollar or two difference when reconciling their accounts at home.

Keeping the Void Authorization card by the terminal negates the entire voiding oversight process. It is so simple for a server to process an order for food, give it to the guest, receive a cash payment, and then void the transaction. In addition to cashiers, some restaurants use two servers per table. One takes the order, one brings the food, then the cashier takes the money. This is a good system.

Supervisors need to be on the floor watching employees, not in the back doing scheduling. Urge your Restaurant managers to watch for fraud.

There are many other ways to defraud a restaurant. If you are interested in more, find one of the many books by surveillance professionals or even the servers themselves. The credit card companies have a vested interest in this process, so follow their procedures and most fraud is prevented.

Do not forget to include your kitchen team. Employees stealing food is common and comes in various forms. Employees picking food off the line, leftovers from guests, or just lying around in the kitchen must be mitigated by management and simple polices.

Unless you provide it as a benefit, do not let employees eat in their own restaurant. Every time an employee consumes a 20 dollar dinner from your menu, the restaurant loses about $13. Employees who are allowed to take home leftovers should be monitored. This can be abused to the point where they create leftovers by cooking up a couple extra steaks or whatever.

Speaking of steaks, who watches the refrigerator? We count, inventory, and lock energy drinks and beer bottles, but we have $50 pieces of meat and fish in the ref that may be unchecked. Is there an inventory on that? If the chef burns one, does he just go get another? This is an area of huge loss. If the restaurant sells eight lobsters and there are ten missing from the ref, who investigates? Likely, it is assumed they were bad or burned or sent back.

More serious is the wholesale theft of food products (and utensils) from the kitchen and storerooms. This is the sous-chef's responsibility and can be controlled through proper documentation of supply use. Treat the food the way you treat money and you will have stronger policies and less loss.

Employees should be reminded when they are hired that unattended food is not free for taking. Do not allow purses or bags in the kitchen. Lockers should also be out of the merchandise area.

I had an executive chef that was taking dishes, appliances, pots, pans, and utensils home every day to subsidize his own catering business. Who is watching that guy?

BARS

Make sure you read the section on nightclubs and restaurants as there is a substantial overlap of these three types of revenue centers. Because of that, this short section will focus on the bar itself.

There are two assets at a bar: drinks and money. Some of the same credit card scams from the restaurants apply to bartenders as well. But there are other unique ways a bartender can add to your losses.

Over-Pouring

Over-pour is a term we use to describe a drink that is served with too much alcohol. An alcoholic beverage is formulated with a certain amount of alcohol, juice, mixers, and ice. These have to be added in the right amounts or the drink is incorrect and the profit margin is reduced. Bartenders, who think they know how to meter a shot, are often mistaken. Plus, it is in their best interest to pour a stronger drink because it will likely add to their tip.

Proper training, documented drink recipes, and supervision are necessary to reduce losses of alcohol. There is technology that helps with this as well. Bar guns can be set to meter amounts and pour spouts can be manually or electronically metered. There are other portion control devices and inventory control systems. The cost of these investments must be weighed against the loss. In addition to the monetary loss, there may be liability for the bar in providing drinks that get someone drunk quicker without their knowledge.

Over-Serving

This is not related to stealing but getting someone intoxicated or getting them drunk faster than normal. One who over serves is one who gives too many drinks to the same person. This can be controlled in a couple of ways. First, a policy should be enacted that requires each customer to get their own drink. Unfortunately, in a busy bar someone, who waited at the bar for 30 minutes, will buy themselves multiple drinks so they do not have to wait in line again. It also is logical that one person might purchase drinks for each person in his group. While it should be strictly enforced, the bartender needs some discretion, such as if he sees the patron's friends where the drinks are going. A beverage server can also help eliminate this problem.

Serving someone who is intoxicated is against the law in most places and is the responsibility of the bartender. That is why one drink per customer is so important. The bartender will keep mental track of how many drinks he gave to one person over how many hours. The rule of thumb is one drink per hour.

Over-serving is a reason we use door hosts. They are the second layer of catching intoxicated patrons. First, they will keep intoxicated persons from coming in, which puts everyone on an even par with the bartender. Second, they will ensure that anyone leaving intoxicated is supervised and gets home safely. Develop a practice of over-serving and you may face fines and license suspension, but even worse you may be held responsible for the unfortunate actions of the intoxicated person who was last seen at your bar.

Over-Charging

Bartenders can manipulate prices on drinks without much deception. Charging for a top-shelf liquor and using a well brand can earn the bartender a buck or two, which will add up by the end of the shift. There may be drink specials that the bartender does not tell the patron about. The patron orders the special, pays full price, and the bartender gets the difference. Same with happy hour prices. In fact, if the bartender knows that no one is checking the point-of-sale records, he may charge happy hour prices all night long. (Many alcohol oversight agencies do not allow discounts on drinks for that reason.) Comps, if you have them, are also easy to manipulate. Simply charge the customer and ring it up as a comp.

The difficulty for the bartender is pocketing the cash. He does not want the customer or the manager or camera to see him pocket money, so generally it has to go into the till with the rest of the money to be removed later. The remainder of this difficulty is knowing, at the end of the shift, how much extra he put in the till. So, what an experienced thief will do, is use some sort of counting system like paperclips or toothpicks, shot glasses or whatever. That is a clue for you to catch a thief.

If a bartender does not calculate his thievery correctly in the till, he will be over. An overage is just as bad as a shortage for this reason. As usual, tight policies will prevent this part of the scam. Keep tips away from the till. Have bartenders tap the bar when they get a tip. (This helps if you use camera surveillance.) Do not allow them to count down and balance their own banks at end of shift. This is called a blind drop and prevents the employee from manipulating the cash to balance with the revenue.

My colleague Russell Kolins has some security measures relating to alcohol service that overlap with mine, but also include CPTED, which was introduced in Chapter 6.

By Russell Kolins

There is a basic design conflict between the need of licensees and their staff to be able to monitor the behavior of customers and the preference of many customers for a secluded area for themselves and their friends. Open-plan designs often meet the needs of the licensee but fail to satisfy customers. Optimal designs may include an open-plan space that is divided in such a way that groups of customers are visually, or psychologically, separated but the licensee and staff can monitor the activities of everyone in the bar: Solid partitions where they do not obstruct the licensee's view, trellis or mesh partitions where blind spots would otherwise be created and differentiated lighting effects (Health Promotion Agency [HPA], 2015).

Where blind sports are inevitable, many licensees and their staff favor the use of carefully positioned decorative mirrors rather than more obvious security devices. However, video surveillance cameras with a monitor behind the bar is also an option which is increasingly used if separate rooms or mezzanine floors are provided, the use of video surveillance is even more important to consider (HPA, 2015).

Whether you are involved in a hotel, motel, resort, nightclub, bar, restaurant, entertainment venue (regardless of size), event locations, bowling alleys, or any other place of assembly that offers hospitality, the following applies to you.

CPTED Concepts

First-generation CPTED deals with the physical concept of reducing crime, fear, improving sense of order, sense of pride and sociability, and fostering sustainability.

Second-generation CPTED identified the social aspects from physical CPTED, but for the sake of this book, you'll be able to discern CPTED as it applies to your industry. There are quality schools and training programs as I mentioned earlier if you are interested in the full-scale CPTED approach to crime prevention. There are intermediate and advance classes on CPTED taught at several universities by current experts.

The purpose of this chapter is to raise awareness, provide a common language, address multi-disciplined teamwork, and to encourage consideration of social and economic factors.

CPTED Basic Principles

Natural Surveillance
Access Management
Territoriality
Facility Maintenance
Order Maintenance
Activity Support

Natural Surveillance

Simply stated, regardless of the type of venue, whether inside, outside or both, the environment must provide maximum ability for monitoring and management. This especially applies to venues that serve alcohol which exacerbates the risk of aggression.

Surveillance should be conducted by humans at all times which includes management, all staff, security, and in some venues, police. Maximum visibility makes undesirables uncomfortable while at the same time gives confidence to desirables, in other words, "*see and be seen*."

Surveillance should also be augmented mechanically. When properly designed in the planning stage, architects working with a team involving security professionals will maximize natural surveillance. However, sometimes the design will be a bit more complex where separate rooms and restrooms create a maze, thus creating the need to adjust natural surveillance methods. Note: if you are planning to design a new venue or renovate an existing venue as seen on Bar Rescue, you would be prudent to consult a security professional to assist your architect in the design phase. There are many well-qualified security practitioners who can be found through the International Association of Professional Security Consultants: www.iapsc.org.

It is highly recommended that you do not depend solely on an architect for security design. It must be a team effort of professionals in their respective fields.

Buildings that were designed without benefit of natural surveillance will apply the same adjustments as will a newly design complex layout. This requires the use of mechanical devices such as surveillance cameras, monitors, and lighting. Locks, door alarms, and signage may also apply. Mirrors, although not mechanical, fit into this category of surveillance as well.

Access Management

Access applies to both coming and going, or ingress and egress. Under CPTED, it is the guidance of those persons which corresponds with natural surveillance. Access management also applies to vehicles, parking lot, and other parking means used by patrons. The strategy is the judicial placement of signage, entrances, exits, fencing, landscaping, lighting, and crowd management to and from a facility. Access management also requires the use of a comprehensive way-finding system particularly in the event of an emergency evacuation requiring availability of optional routes so pedestrians can avoid undesirable encounters.

Visibility is critical for effective emergency movement. A proper emergency evacuation plan was discussed in Chapter 7.

Territoriality

The use of boundaries that show pride and ownership of the space and defines an area of influence.

Facility Maintenance

Well-maintained facilities attract people and keep them straight. Broken lights, tables, chairs, mirrors, seats, and other furniture should be replaced or repaired before the next business day. Clean bars, restrooms, tables, floors, windows, fixtures welcome acceptable behavior. This ties into the "Broken windows" theory that is briefly discussed in the previous chapter and mentioned elsewhere in this book.

Order Maintenance

This addresses quality-of-life issues that are good for business and bad for crime. Strategies include using graffiti resistant materials, immediate repair of vandalism or breakage, clearly defining the hours of operation conditions of use for vehicle and pedestrian routes, and locating formal gathering areas where guests may be easily observed such as a dedicated smoking area outside and away from the entrance.

Activity Support

Provides clear border definitions and adds eyes internally and externally on the street.

According to the Portman Group (2000), the aim when designing a licensed premises should be to meet reasonable customer expectations, and achieve an optimal balance in terms of stimulation, to provide an environment that maximizes ease of monitoring and management and to avoid spaces that serve as "poser platforms" for my Choate display.

Bar characteristics themselves may promote violence. High temperatures, poor lighting, ventilation, noise, etc. have been found to be related to bar violence (Graham, 1980). Crowding around the bar area creates the risk of accidental bumping and irritation that can also lead to conflict (Scott and Dedel, 2006).

Add alcohol to the equation, it's a recipe for disaster. Poor bar layout and design within crowded premises increases the potential for aggression to occur (Institute for Alcohol Studies, 2010).

Frustration arises when customers are prevented from doing what they want or getting what they expected to and if triggered in some way, can result in aggression (Portman Group, 2000). Frustration is often directly linked to design factors including insufficient bar serving areas, poor layout, inappropriate temperatures, sound and light levels, poor quality fittings that are easily damaged, and fittings in toilets that are easily vandalized or damaged. The solutions to many of these problems can be simple and cost-effective according to the Portman Group.

A comfortable and entertaining atmosphere reduces both frustration and boredom among patrons which can reduce aggression levels. Attractive well-maintained bars and other venue type suggest to patrons that the owners care about their property and will not tolerate disorderly and violent conduct that might destroy it (Deehan, 2004). The CPTED principle that Deehan addresses here is territoriality.

It Starts with a Plan

Before getting to territoriality, there has to be a plan. The design phase or redesign phase requires understanding vulnerabilities that lead to identifying risk. The initial assessment is the vulnerability assessment. The new CPTED ISO 22341:2021 defines vulnerabilities as the "the opportunities for negative effects and the lack of maturity related to the effectiveness of the associated countermeasures."

A security plan should be based on a security survey, like the Risk Assessment discussed in Chapter 1. The security and fire life safety needs of any facility are determined by identifying specific assets, the threats against those assets, and the risk of those threats materializing. The purpose of a security survey (Security Vulnerability Assessment) is to ascertain the present security status, to identify deficiencies, to determine the protection needed, and to make recommendations to improve the overall security.

"A security survey is essentially an exhaustive physical examination of the premises and a thorough inspection of all operational systems and procedures. Such an examination or survey has, as its overall objective, the analysis of a facility to determine the existing state of its security, to locate weaknesses in its defenses, to determine the degree of protection required, and ultimately to lead to recommendations for establishing a total security program. In the process of risk analysis that proceeds from threat assessment (identifying risk) to threat evaluation (determining the criticality and dollar cost of that risk) to the selection of security countermeasures designed to contain or prevent that risk, one of the management's most valuable tools is the security survey" (National Fire Protection Association 730).

Tavern, nightclub, and event venue management should first identify and assess the risks to their establishment, including any violence during the last few years at the club, and to a lesser extent, the violent crime history in their immediate neighborhood and at any nearby venues, bars, and clubs. Management should then develop its security plan based on the type of customers they attract, plus the known or likely risks or problems. A key factor is knowing your guests/patrons—who are you attracting? Written plans are always preferred, especially for training, continuity, and documentation purposes. This was addressed in an earlier chapter.

Once the potential problems and risks are identified, countermeasures (policies, procedures, personnel, and equipment) can be developed, and personnel trained in their implementation. Owners and managers should take care to staff their establishment with responsible, trained employees in all positions. The security plan should be reviewed at least annually, or more often if problems are occurring, to determine whether any changes in the security plan are needed. Most importantly, all staff, especially security, should be trained (with the training documented) so that they understand the goals, policies, and procedures of the establishment. Employees implement policies and procedures, with direction, guidance, and supervision by management.

The hiring of qualified and trained security representatives serves as mere presence, is a deterrent, and are extra sets of eyes for the management. This, in part, is the Activity Support CPTED principle. A security representative, when positioned correctly, "*is an additional factor in identifying, thwarting, or dissipating a dispute, as time is of the essence.*" The second goal of a security representative is to "*intervene if deterrence fails.*" The security officer's goal in any potentially violent situation is to defuse the situation, not incite a physical confrontation. To achieve this goal, the security officer must be proficient at recognizing or assessing potentially violent behavior. He or she must learn to use verbal skills that minimize the risk of agitating the potentially violent individual. He or she must also learn how to use only non-offensive physical techniques, and when it is appropriate to use them. Natural surveillance allows for quicker response time. Of course, control of the patrons by design and other CPTED measures contributes to a more even flow of acceptable behavior.

A study of *Assaults in and Around Bars* conducted and published by the United States Department of Justice, Office of Community Oriented Services, found the following factors, in part, contributed to aggression and violence in bars (Scott and Dedel, 2006):

Alcohol—Drinking alcohol is the most obvious factor contributing to aggression and violence in bars.

Culture of Drinking—Cultures that are more accepting of intoxication as an excuse for antisocial or aggressive behavior, and that relaxed the normal rules of society during drinking time, have higher levels of violence in and around bars.

Continued Service to Drunken Patrons—This, of course, is in direct violation of state law and has no excuse for lack of alcohol management.

ISO 31000, "RISK MANAGEMENT" defines risk as the effect of uncertainty on objectives. In a security context, risk is composed of three elements: assets, threats, and vulnerabilities. Crime and security risks are based upon the value of the asset in relation to the threats and vulnerabilities associated with it. This approach can be viewed as an operational implementation of the risk management standard with a specific focus on crime and security risks. Threats and vulnerabilities influence the likelihood dimension and assets influence the consequences of a risk.

Threats are the potential offenders or hazards and should be addressed by identifying the nature of the threat which can be done by:

- focusing on the most likely scenario being addressed as a narrative;
- describing the subject of the scenario;
- describing the who (the offenders), where (the place of the offense), and how (what means used).

ISO 22341:2021 further defines vulnerabilities as the opportunities for negative effects and the lack of maturity related to the effectiveness of the associated countermeasures.

The crime and security risk are greater when a motivated offender and suitable target come together in time and place, without appropriate countermeasures present. The countermeasures would be human security, the built environment, and mechanical measures described earlier in this chapter.

To mitigate the opportunity for a crime to occur, the conventional approaches are followed to remove one or more of the factors expressed in the crime and security risk triangle. Crime events require these three factors to all be present at the same time:

- assets (suitable targets)
- vulnerability (lack of capable guardianship/countermeasures)
- threats (criminal offenders)

Capable guardianship is the willingness to supervise, detect, and take action to prevent or discourage the occurrence of crime. In order to accomplish an effective security plan, there must be policy, procedure, training, supervision, and enforcement of the policies. This and an understanding of CPTED security measures combine for a successful operation, reduction of crime and fear.

Training includes situational awareness that enables security to identify threats in advance and to mitigate the threats timely. As stated earlier, it's all about "prevention." Basic security principles according to ASIS International are Detect, Deter, and Delay. We add an "R" for Respond. Detecting a threat, timely response to the threat, and removal of the threat spells "prevention."

> Training itself is a policy issue. Supervision and education of managers and servers and security staff are important functions of the licensee. All servers, supervisors,

> and managers and security staff act as an agent or servant of the licensee and it is the licensee who is the one responsible under the rules of agency.
>
> *Fay 2007*

It is well-established that the proprietor of business premises has a responsibility to its patrons to provide a reasonably safe place to do that which is within the scope of the invitation. To this end, there is a heightened risk of danger and harm in the retail alcohol business because of alcohol consumption. Licensees, through their management and staff, should always expect the unexpected and take reasonable measures to protect patrons, guests, and employees. It doesn't matter if the business is a mom-and-pop shop or a major concert venue owned by corporate conglomerates.

Policies are fundamental to server training programs whether in a bar, nightclub, casino, hotel, event venue, bowling alley, and any other place of assembly that serves alcohol.

> Without responsible establishment policies in which to put server training into practice, the establishment's responsible business practices lose significance. Without establishment of specific policies, servers and security staff indoctrination in responsible procedures are separated from supportive and objective standards on the job. Responsible licensees do not permit themselves or their licensees to be put in jeopardy either by the absence of policy, by policies that permit or encourage irresponsible drinking, such as open bars or such as policies that ignore liability risk exposure
>
> *Scott, 2006*

Training and adherence to the law and regulations serves not only to protect the patron but also serves to protect the owner and staff. Understanding through training and adherence to these regulations strengthen the employees' understanding to prevent underage drinking.

Simply stated, a proprietor is responsible for providing reasonable care to its patrons to provide a safe and comfortable place in which to do business. It has an obligation to take steps that are reasonable and prudent under all circumstances relevant to a patron's safety. The obligation requires the owner/operator of a bar or venue to exercise ordinary care to protect patrons from potential injury from serving a customer displaying signs of intoxication and to take steps to assist the patron with a safe alternative to get to a destination.

CPTED principles were designed to help facilitate as many issues that can be expected to arise in any facility or venue. Natural surveillance allows for observation of persons who have consumed more alcohol than they should have which could contribute to acts of aggression or that person's safety and/or any other person he or she could potentially victimize if allowed to drive while intoxicated. There are other issues with persons who are intoxicated such as a person falling down stairs or maybe stumbling in front of the speeding car while crossing the street. Regardless of the potential threats, as stated in the previous paragraph a proprietor is responsible for providing reasonable care to its patrons to provide a safe and comfortable place in which to do business. All staff, including security, should have a basic familiarization regarding alcohol management and the effects of alcohol. Some states have proprietary alcohol management training programs, but the most recognized in the United States and abroad is the TIPS Program. On-Premise training programs are designed for Commercial, College, Casinos, Package Goods stores, and more.

The TIPS ("Training for Intervention Procedures") program was developed by the Health Education Foundation of Washington, D.C., under the direction of Morris Chafetz, M.D., with the assistance of numerous other doctors, lawyers, and experts in the alcohol and hospitality fields. The TIPS for On-Premises program is designed to teach participants acceptable standards of practice for serving alcohol.

TIPS is the generally accepted standard in the retail liquor industry which should be followed by all owners, management, and staff, from the owner to the busboy, who are inside the premises, and valets, who work the outside.

Bartenders/servers are trained to look for changes in people's behavior after a few drinks, which are called "*Behavioral Cues*." Usually, the more alcohol in the bloodstream, the more obvious the cues. Cues are exhibited in four areas:

Inhibitions: Becoming talkative, displaying loud behavior or mood swings, or exhibiting a notable change in behavior can all indicate lowered inhibitions;
Judgment: Behaving inappropriately, using foul language, telling off-color jokes, annoying others, becoming overly friendly, or increasing the rate of drinking are signs of impaired judgment;
Reactions: Glassy, unfocused eyes, talking and moving very slowly, forgetting things, lighting more than one cigarette, losing one's train of thought, and slurred speech result from slowed reactions;
Coordination: Stumbling or swaying, dropping belongings, and having trouble picking up keys, change, or other items can indicate a loss of coordination.

TIPS also teaches intoxication rate factors, which help servers and security staff to assess how quickly someone is becoming intoxicated, presenting the idea of how rapidly that person's blood alcohol is rising. Intoxication Rate Factors are an important issue in all recognized responsible alcohol management training programs. According to the TIPS Training Manual, these factors help a bartender/server assess how quickly a person will become intoxicated and can give the server an idea of how rapidly that person's blood-alcohol content (BAC) will raise Intoxication rate factors, which are:

Size: Smaller people are typically affected more quickly by alcohol than larger people. However, larger people with a high percentage of body fat can become intoxicated faster;
Gender: Women are generally smaller, have more body fat, and tend to reach higher BACs more quickly than men;
Rate of Consumption: Gulping drinks and ordering frequently will increase the amount of alcohol taken into the system;
Strength of Drink: Drinks of different types (e.g., straight, carbonated, or juice mixer) have varied effects based on their content;
Drug Use: Legal or illegal drugs can speed up the effects of alcohol and have an unpredictable outcome;
Food Intake: A full stomach before or during drinking slows the absorption of alcohol into the bloodstream.

To understand BAC, key points to understand are:

The more alcohol a person consumes the higher the BAC level will be;
A guest's BAC level can be different each time he or she drinks;
Intoxication rate factors affect how quickly the BAC level rises;
The higher the BAC level, the more behavioral cues you are likely to see;
Time is the only thing that can lower a person's BAC level.

Bartenders/servers are taught a guideline using a 150-pound male guest drinking for one hour on an empty stomach, who would likely have the following BAC levels:

two standard drinks equal .05 BAC
four standard drinks equal .10 BAC
eight standard drinks equal .20 BAC
twelve standard drinks equal .30 BAC

Trained owners, managers, and servers learn that alcohol server standards calculate a standard drink measured as ½ ounce of ethyl alcohol. This is the equivalent of:

1.5 ounces of 80 proof spirits or
1 ounce of 100 proof spirits or
5 ounces of table wine or
12 ounces of beer.

Behavioral cues are but one way to gauge whether or not a person is visibly intoxicated or being served in such a manner that visible intoxication is inevitable.

Security must also be trained regarding the use of date rape drugs and be on the lookout for female patrons being escorted by a male or males. This is all the more reason for natural surveillance. But, if a female falls victim to such a drug and is virtually being dragged and held up by the offender, there must be a challenge by security and management to evaluate and determine the actual situation.

Every type of venue has restrooms which are known in the industry to be one of the major security threats. They are vulnerable to drug activity, assaults, and sex crimes. When no attendants are present inside the restroom, security should be posted in the entrance area as a deterrent to restroom criminal behavior. Drinks and glasses or bottles should be prohibited and security should conduct periodic checks as a means to remove threats associated with restrooms.

Threats are attached to every phase of the hospitality and entertainment venues in many ways. Another common major threat occurs during the closing or on the sidewalk and/or parking lot vulnerable to violent behavior. Proper lighting, video surveillance, police and security patrols during this period can be a major deterrent to assaults and other criminal behavior.

Quality lighting in parking lots, alleyways, and public external areas will discourage loitering and reducing groups of persons who create a threat of violence and criminal behavior. Good lighting as a CPTED measure denies offenders the ability to operate unobserved. It is important to note, however, that no one CPTED security measure can deter all bad behavior. Depending on the area and threat, other security measures should be applied. Parking lots for instance may require human presence like police and security or other mechanical devices such as video surveillance cameras that are obvious to potential offenders. Remember, parking lots are for parking, not for loitering.

Restroom design has changed over the last few years. New design of ingress/egress has eliminated doors. People can now walk in and leave without having to open a door. A partition provides privacy. This is a CPTED measure that allows security to advance an inspection without warning by opening a door. It also creates the ability for someone outside the restroom to hear screams for help that ordinarily would be muffled by a closed door.

Crowding often contributes to alcohol-related aggression and violence. Other factors contribute to aggression and violence such as warm temperature, noise, and levels of intoxication. We discussed that alcohol lowers inhibitions and also lowers tolerance to social and environmental irritants. Crowding also interferes with the ability of staff to monitor for intoxicated patrons. While local fire marshals use a formula to determine the maximum number of persons permitted on a premises, management and door staff can play a key role in determining a lesser number based on factors such as temperature, type of crowd and activity.

Internal lighting can play a significant role in creating the right atmosphere. Extremes of lighting, such as being too bright or too dim, should be avoided. Very bright lighting is cold and unwelcoming for patrons. Whereas, lighting which is to dim makes it difficult for bar and security staff to monitor the behavior of customers effectively, particularly for the signs of intoxication and for checking IDs.

There may be a need to break up large, open areas into smaller units. Directional lighting, which creates pools of light interspersed with less brightly lit areas, can help to achieve the effect of divisions. Installing dimmer switches increases control of areas from behind the bar. An override allows, in the case of an incident occurring, the lighting level to be raised and is an important element of control. This will also assist at the end of the operating hours that patrons are easily made aware that the premises are closing (HPA, 2015).

Outdoor drinking areas have become increasingly popular, especially as a result of the pandemic. In many cases, outdoor drinking areas cannot be seen by the staff working inside a liver proper monitoring of patrons in these areas should be carried out frequently by bar and/or security staff. This can also be suitable for video surveillance which must be monitored as an action component by a human.

Entrances and exits play an important role in reducing opportunities for crime. It allows bar and security staff to monitor who is entering and leaving the premises. Entrances including emergency exit should be easily viewed from behind the bar or serving area. If this is not possible, use of video surveillance should be considered to monitor blind spots. It may be best to minimize the number of entrances although this must be in accordance with fire safety and life safety requirements. Where door staff are for use, space should be provided for them so as to avoid congestion in the doorways, which can lead to conflict. This area should be covered with good lighting to assess those entering and leaving. Where customers may need to queue to gain access to the premises, there should be sufficient space so that those queuing do not obstruct the footpath of other patrons in line or close by businesses (HPA, 2015).

Space in this chapter is limited. Not every design, nor every risk, vulnerability, and threat scenario can be addressed here. The intent is to give you a brief understanding of what CPTED is, how you can implement it, and how it can benefit you effectively without breaking the bank.

Effective management of licensed premises involves the following punctuation (HPA, 2015):

> There are sufficient numbers of staff, particularly management and security staff to manage the volume of people and any potential problems.
>
> There are sufficient numbers of bar staff to avoid customer frustration and waiting to be served.
>
> Staff are proactive in encouraging patrons to seek assistance if they experience offensive or aggressive behavior. This may include signage encouraging customers to report any bad behavior. See something, say something.
>
> Staff are trained to deal with complaints positively rather than dismiss them.

Security staff may be a positive or negative factor in the incidence and severity of harm arising from aggression and violence. A number of studies have found that security staff contribute to a high proportion of violent incidents (Doherty & Roache, 2003). They were witnessed either creating violence, using excessive physical force, shifting the problem to the street and observing or participating in the continuance of violence.

Security staff should therefore be properly trained and certified for their role and possess good conflict resolution and crowd control skills.

The following checklist applies all of the CPTED principles described in this chapter. Special thanks to the Health Promotion Agency (HPA) and New Zealand Police.

CPTED Checklist for Venues that Serve Alcohol—Bar Area

> Bar staff have good visibility of entire premises
> Area behind the bar is raised to improve visibility
> Bar area is open with no obstructions affecting monitoring of premises
> Cash registers are front facing. If cash registers are not front facing, mirrors are installed for monitoring members and their guests
> Safe is out of public view

Internal Layout

> Premises is laid out so staff can monitor all members and their guests at all times
> There are no obstructions within the bar causing blind spots
> Where there may be blind spots, mirrors or CCTV are installed
> Bar is easily approached by members

Sufficient seating is provided
Members and guests cannot climb on structures or fittings
A ventilation system is installed
Premises are maintained at a suitable temperature

Crowding

The premises are not overcrowded
The maximum number of persons for the premises is displayed and followed

Lighting

Internal lighting is suitable
Lighting allows bar staff to check IDs etc.
Lighting allows staff to monitor members and their guests inside the premises
No areas are too dark inside the premises
Internal lighting can be raised in an emergency or incident and at closing time
External lighting is suitable
External security lighting is installed

Outdoor Drinking Areas

The premises are maintained at a suitable temperature
Outdoor drinking areas are monitored by bar and/or security staff
Lighting allows staff to monitor members and their guests
Outdoor drinking areas are well defined from surrounding external environment
Outdoor drinking areas are not overcrowded

CCTV

CCTV is installed
CCTV is positioned to monitor vulnerable areas
Members are aware of the CCTV system
Staff understand its operation

Entrances and Exits

Entrances and exits are visible from behind the bar area
CCTV is installed to monitor blind entrances and exits
Door staff monitor entrances and exits
Toilet facility entrances are visible from the bar area
Toilets are inspected regularly

Staff

There are sufficient numbers of staff to ensure control of the premises
Staff are visible to members and their guests
Staff monitor the premises for conflict and crime
Security staff are properly trained and certified

RETAIL

Policies

Most hotels have some sort of retail footprint from a kiosk of sundries near the Front Desk, to a full-blown shopping mall. Retail has become an important revenue source for most hotels, surpassing some of the traditional generators. It is vital that you establish strong loss prevention policies in this area to protect the physical assets as well as the safety of guests and employees.

Shrinkage is the amount of goods lost in a retail environment due to theft or breakage for which there is no reimbursement. Loss can include shoplifting, employee theft, damage, inventory errors, and so forth. In a hotel, the first consideration will need to be who is responsible for protecting against shrinkage. A store that leases space may be responsible for its own merchandise and employees. Or it may rely on Security to provide this function. Either way, it needs to be worked out in writing, in advance, because your officers will need to be acting as an agent of that company when making arrests or conducting investigations. If the store is owned by the hotel, then your umbrella will extend over that store as it does over all the other amenities on the property.

Retailers accept a certain amount of shrink as part of doing business. The national average runs about 1.5% of sales, which means $1.50 is lost for every $100 in sales. Find out from your retail manager what their shrink is. If it is higher than average, there may be some unacceptable theft going on, or mismanagement of operations. As with walkouts and room losses, we need to decide whether the problem is criminal or administrative and then whether we want to prosecute someone for shoplifting.

Shoplifting is what we commonly call petty larceny in a retail environment. (Theft by employees is different and is addressed later.) Petty larceny is defined by state law in most cases and is the taking of property with the intent to deprive the owner of that property. Both of these elements need to exist for a crime to occur. Larceny can be grand or petty depending on the amount of goods taken and that varies by state. There may be some other covenants associated with this crime, so make sure you are familiar with them. Some larcenies may be burglaries depending on whether you can prove the suspect's intent, certain tools used for the crime, etc.

Shoplifting

Larceny, as mentioned previously, requires the intent to deprive. That is why you generally don't stop a suspect before he gets past the register or the door because of the doubt that the person intended to pay for the item. Most shoplifts are misdemeanors, and in most jurisdictions a private person needs to witness the crime in order to make an arrest. This makes loss prevention more difficult because you cannot stop someone just because you think he put something in his pocket or you are pretty sure he hid something under his jacket. Some states have created retail loss prevention laws that allow security to stop and question someone whom they have reasonable suspicion to believe committed theft. This is a touchy situation, as it does not necessarily allow you to arrest or search the person.

Catching Shoplifters

Because of the restrictions just explained, which are really an extension of the Constitution, it is difficult to catch thieves in the act. Prevention is much easier and is discussed shortly. Retail loss prevention officers are a special breed and they seem to have a sixth sense for knowing who is going to steal. You cannot watch every part of the store or every shopper, so it can seem like looking for needles in a haystack.

Profiling, or behavioral recognition, is the first step in identifying a shoplifter. Of all the people entering the store, who is most likely to steal? This depends on your hotel and the environment. The obvious physical characteristics might be someone dressed as a transient, a local resident in a tourist hotel, teenagers, and persons with heavy jackets in the summer. There is no physical profile that addresses gender, race, or age because shoplifters cut across all of these demographics, so concentrate on behavior more than appearance. Notice shoppers in any store. There are browsers and those who know what they want. Either way, both types generally focus on the merchandise. A potential thief concentrates on his surroundings. He may be looking for cameras, clerks, other witnesses, or his lookout. This is called "rubbernecking." Some will eye their target and immediately grab it, and some will position it on the shelf, try to appear disinterested, and then come back to it when the coast is clear.

Your policy on shoplifting is going to depend on several factors. Do you have security onsite? If not, there is no way you are going to apprehend or hold a shoplifter for the police. What is your pursuit policy? Presumably, you will not chase someone who steals from your store. This is dangerous and has resulted in injuries much more serious than a theft.

How will you know they have stolen? The professionals that prevent loss at Department stores and big-box chains use someone watching video and another agent approaching the suspect. This is, again, dangerous, costly, and troublesome legally.

Make sure cashiers are trained to react to a robbery. (Do as the suspect says, be a good witness.)

It is better to prevent the thefts than react to them. Locked displays, inventory control systems, staffing, and other measures provide deterrents over detection, which is always more economical.

Whatever you do to prevent threats like these on your property, keep in mind two basic tenants.

(1) Do not reinvent the wheel. Every other property experiences the same issues as you. Network and get some ideas if you have none. (2) Procedures are easier to enforce, less costly, and generally proven. So before you go out buying gadgets and hiring more staff, check your methods and documentation first.

A good loss prevention officer spends much of his time on surveillance. There is physical surveillance, which means walking the store undercover, and visual surveillance, which means using cameras or mirrors and blinds. A blind is a two-way mirror, catwalk, or hidden area. Loss prevention officers often work in teams with one officer at the entrance, profiling people as they enter or patrolling the store. The second officer will be working the cameras. Each officer communicates with the other, pointing out suspicious behavior. When a crime is observed, they will intercept the thief at the door.

Arrests

Whenever you put your hands on anyone, regardless of the justification, you have just exposed yourself to great liability. Besides the risk of making a false arrest, and injury during a struggle, you now are responsible for that person and anything that happens to them will be your fault.

In 2009, two loss prevention officers working at a well-known home electronics store chased a shoplifter out the doors and into the parking lot. The suspect pulled a knife after being tackled and threatened the officers to make his escape. He got away and the men were summarily fired for violating corporate policy on off-property pursuits. Most companies have strong policies on pursuits and arrests because of injury liability. The chances of the employees and even the suspect being injured running through the parking lot are extreme, and not worth the value of the lost merchandise. In this case, the employees could have been murdered, resulting in a much more serious loss for the company and the employees' families than some hi-fi equipment.

Nobody likes to let the bad guy get away, but we need to look ahead and think of the big picture when creating and enforcing policies like these that keep our liability at a minimum.

Many national retailers now have policies that forbid or restrict arrests for shoplifting. Others allow the arrest as long as it does not involve a pursuit. We hate to let someone get away with theft, but compare the cost of a stolen CD to the price of a lawsuit, even if you win. Your policy will need to weigh the value of the arrest—deterrence effect, hotel reputation, labor cost—with the value of letting the person go.

Preventing Shoplifting

Like everything else we do to protect assets, prevention is more effective and cheaper than trying to catch criminals. There are several things we can do in the retail environment to prevent shoplifting.

Retail Staff Training

Our best defense against thieves in a store is the clerk, cashier, stocker, and manager. These employees must be given basic training on loss prevention and guest service. They are actually the same training, if done right. The following are suggested training points that your retail manager will love.

Greeting—Every person who enters the store should be greeted and given eye contact. Besides the obvious service value, this tells the thief, who wants to go unnoticed, that he was noticed. The eye contact forces the clerk to remember the person's face and to unconsciously do some behavioral recognition of his own. Workers in a store know which visitors are going to steal.

Follow-up—This separates the two shoppers we identified earlier. The "browser" from the "targeted." The guy who wants a bottle of aspirin goes right to it, gets it, pays, and leaves. After the browser has passed a couple of displays, the clerk says, "May I help you find something?" or "Did you know these are on sale?" This reminds the shopper that we are watching, we haven't forgotten about him, and it is unlikely he will get away with stealing something.

Clerk patrol—The clerks should be walking the floor as much as possible. When there is no transaction, they should be cruising the store, providing that follow-up. During transactions, they need to be trained to lift their head from the register and make an occasional sweep of the store with their eyes.

Communication—There needs to be a method for the clerk to alert Security or Loss Prevention of a suspicious shopper. Maybe it is a silent alarm button, a discreet phone call, or body language that tells the manager to watch that person. There may be a different signal if they actually witness a crime. Remember, we cannot stop someone unless we witness it, so what do we do if the cashier witnesses it? Have a plan to act as their agent and make the stop, but it has to be a solid communication. You do not want to chase a guy down and stop him only to find that the clerk just thought he looked suspicious.

Store Layout

This is a conversation you need to have with the store manager. Remember our Risk Assessment? This is where it is used. Most retail professionals know how to lay out a store to maximize floor space, provide the best visual sales, and protect merchandise. But sometimes they forget that last one about protection. Once you have made your assessment, sit down with the manager and review your concerns. They should be willing to cooperate with this mutual concern.

Layout of displays needs to account for ease of shopping for the customer, but also for good sight lines between the clerk and the customer. Smaller, more expensive items need to be near the register; larger items should be toward the back and in the blind spots. Consider a layout where the register area has a clear view down each aisle. The retail manager can meet your needs as well as his own with this configuration. Convenience stores have definitely figured this out and are a good resource.

Cameras and Mirrors

In order for cameras to prevent crime, they need to be visible, but not obvious as to their view. Dark bubbles are best because it is assumed that a moving camera is behind the bubble. Mirrors can be used with cameras very effectively. Many retail shops use decorative mirrors around the upper walls of the store, angled down. These mirrors not only allow store personnel to see blind spots, but a skilled camera operator will use mirrors to expand his coverage of the store as well. Mirrors are a relatively inexpensive alternative to having so many cameras.

Antitheft Devices

Antitheft devices are those small tags that are now installed at the factory in DVDs, power tools, cosmetics, etc. These generally work as a radio frequency tag or magnetic sensor. The types and choices are vast and varied, so just keep a couple of things in mind when installing or operating them. First, you need to justify this expense. Maybe you don’t have a big enough shrinkage problem for this to pay for itself or your merchandise is lower value stuff. Second, is shoplifting the majority of the shrinkage problem? Many losses go out the back door with employees and you need to have an idea of what the percentage is.

Also, remember that these devices can be defeated by the shoplifter and by the employee. This will be just one layer of security and will not eliminate the need for other security measures.

Organized Retail Crime (ORC)

Like prostitution, we only see the surface of what is an enormous criminal enterprise. Shoplifting has become sophisticated and each incident is a national event as merchandise is quickly moved across state lines. It also includes credit card fraud, gift card fraud, and other income methods. Unfortunately, the shoplifters know that we limit ourselves to reduce injury. Policies like hands off, no pursuit, and no off-property confrontations are well known and make the crime easier than the express check-out.

A phenomenon that is going strong now is "the pushout." Knowing that they will likely not be pursued, the thief loads a cart with high-priced items and goes right out the main door (or an emergency exit) to a waiting car. The Loss Prevention (LS) guys are standing at the door watching and calling the police. Large stores have used technology to prevent these thefts by installing one-way gates at the entrance, cameras in certain departments, and locked cabinets for the high-risk items. There are also police units dedicated to ORC that gather intelligence and run special surveillance and undercover operations to catch these guys.

There is also still the Flash Mob that was big ten years ago. This is a group of teens, usually that invade a store and overwhelm the staff by grabbing everything they can. The one or two clerks are left helpless as the aisles are decimated. Looting is a similar crime that occurs when the store is closed. What is not obvious is that these folks are often motivated by the ORC folks who will pay them for their crimes or buy the merchandise. That lady who comes out of the Louis Vuitton store with ten purses is not going to sell them on Ebay.

It may seem a little far-fetched to get interested in these crimes from a hotel's perspective, but we can still be involved on a smaller scale. Take some hints from the big retailers as to layout, video, item placement, and so forth. You may also find there is a Law Enforcement/Retail working group for ORC where intelligence is shared.

In 2008, a "swarm" of seven or more black males attacked a landscaper at the MGM Grand Hotel in Las Vegas. The victim was white and the suspects were all convicted of a hate crime. They all belonged to the same gang.

This was not the first crime of its type, but was one of the first recorded on video. It brought national attention to the phenomenon, which became known as Flash Mobs. It was determined during the investigation that the gang used texting to coordinate the crime by arranging a meeting place and time. The meeting place was a nearby retail parking lot. Las Vegas and other major cities have seen the expansion of these events to include other types of venues. The proliferation of social media has aided these groups to the point of including any stranger who wants to attend as an associate.

Credit Cards

We talked quite a bit about credit card scams. There are some additional things you should know about credit card fraud.

The credit card industry—including Visa, Mastercard, American express, etc. have created their own procedures for accepting and processing credit card transactions. These are very strict rules and if not followed, they can fine you, refuse to let you accept cards, and will not cover losses due to fraud.

The opposite is also true. If you follow the procedures, your company will not be responsible for losses. And that is where it gets kind of frustrating for those of us who like catching bad guys. As you know, the credit card company absorbs the loss on a bad transaction (if procedures are followed) and pays you for the transaction. That makes the credit card the victim of the crime. Unfortunately, the credit card company finds it cheaper to take the loss than to investigate the crime, so doing a police report is not only useless, but impossible. You are not the victim.

There are still other ways for the police to charge these criminals, but the actual credit card fraud is rarely charged. So your crime fighting as it relates to credit cards will be limited to making sure your cashiers follow procedures.

You will likely get calls from guests who get their credit card statement and find a charge at your place that they did not make. While you should help them out as best you can, just confirm for them it was fraudulent so they can contact their card issuer and get it removed. Your other objective would be to make sure you do not have a guest in-house on a bad credit card or that an employee did not steal the number and use it.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

11

Employee Awareness

Before 9/11, we really did not put much credence in the average citizen being able to contribute anything to security. But when we looked at all the hundreds of clues that were ignored or missed leading up to 9/11, we thought we better get on it. After all, countries in the Middle East have been performing this vigilance for decades, and they do it naturally and successfully.

When October 1 happened, we were again mortified that something so enormous and "successful" was planned, prepared, and conducted right under our noses and with our help, in many steps along the way. This is no one's fault, except that of the asshole (am I allowed to write that?) that did it. No one should feel bad or guilty, that I know of. His entire motive was to see if he could do it, and he did.

Speaking of motive, everyone has really gotten caught up in the search for a reason with this guy. Let me tell you right now what his motive was: He was crazy! Mass murder, by its very definition is crazy. Just like Manson, Dahmer, and Hitler, he heard voices in his head and that is all there is to it. Unfortunately, or maybe fortunately, we cannot hear those voices, so we must rely on other cues and clues. We need to get better at that to prevent these types of events and I know we can do it.

And another thing, please stop giving this guy credit as some genius or mastermind that circumvented the security in a huge hotel. You or I could have done the same thing, but the difference is we did not. That is what separates normal from daft. Every day we put our lives in the hands of fellow humans and 99.9999% of the time, it works well. Any one at any time can betray this unwritten agreement, but they do not—except for this blankety blank. Let's hope there is a special place for this jerk, down there with Hitler and the rest, and move on to prevention.

In my opinion, we need to change our communication methods and which data gets relayed to stop horrible things from happening. I have seen some great advances in this area, and I have some of my own for us to explore. My first recommendation is to change the culture in the workplace—well, everywhere, frankly. Consider these examples of culture shifts in recent history.

- A woman walks past an abandoned backpack in a marketplace. She alerts her fellow shoppers, and the area evacuates in seconds. The improvised explosive detonates harmlessly.

DOI: 10.4324/9781003037644-11

- A housekeeper at a hotel facing a parade route notices electronic paraphernalia in a hotel room that is inconsistent with a tourist's luggage. Police are summoned and uncover an assassination plot.
- Three men on a passenger jet notice a passenger behaving in an erratic and threatening manner toward a flight attendant. The man is detained by the passengers and taken into custody at the next airport for a terror plot.
- Three military veterans in a foreign country notice a terrorist on a train setting up for a mass attack with a rifle. Instead of "see something say something" they kick his butt, saving dozens of lives.

These actual incidents illustrate what can be accomplished with a change in culture: Helping employees and guests to bear some of the responsibility for their own safety. Technology is going to play a huge role in this new culture, but in the end, I think that it will be humans who save humanity from other humans. So, as I mentioned before in problem solving, let's look at where we are now before we figure out how to get to that level of security.

I am not speaking of your security force. We can train them and get them where we need them. It is the other employees whose senses we need to exploit. They know things, but they just do not know that they know things. Right now, we are showing them a video in new-hire orientation. And we have a bulletin board with some posters. Can we do more? How about these facts:

> Less than 5% of your workforce is focused on safety and security (your security department). Imagine the buy-in if all departments had a responsibility for keeping themselves and guests safe.
>
> Your Valet, Bell, and Housekeeping Staff "touch" every guest every day.
>
> No one remembers anything they were presented in New Hire Orientation except where the dining room is and when do they get their first check.
>
> When was your last property-wide emergency exercise? Cruise Ships, for example, require ALL passengers to participate in evacuation drills on every embarkation. Each crew member has a dual assignment during an emergency.
>
> We still discourage employees from carrying and using their phones on the job, even though it is arguably their best tool for safety.
>
> When confronted with a life-threatening situation, most people will revert to their instincts. A lack of training or practice means most people will freeze while their brain processes a plan.

I think there is opportunity for growth in this area. It does not cost more, really. It is not even difficult, really. Artificial intelligence, for example, is being used far and wide, and maybe at your hotel—for marketing. Casinos in China are taking gaming habits, travel habits, eating and shopping habits, and figuring out how to market to their high rollers. They even know where these players are at any moment—without a tracking device.

Your multi-colored search engine uses the data that you input, sells it to retailers to show you ads on the things that interest you. I know some people way smarter than me are working on this for security, and I praise them for it. Meanwhile, I will give you some more down-to-earth recommendations to use until those guys deliver a useable platform to save the world.

Generally, when an incident occurs, we learn from it. Columbine, Virginia Tech, Paris Nightclub, Fort Hood all brought important vulnerabilities to light and even spawned new technology and techniques for prevention and response. These enhancements tend to counter one threat, but we are starting to realize that we cannot anticipate the imagination or ingenuity of someone that is bent on doing harm. This will require a comprehensive change to the Security Culture.

The See Something Say Something campaign was a great slogan with good intentions. Unfortunately, the objective was not supported by the process, and the process was not understood by the public. Some Security experts have taken this slogan and built training programs and technology around it in an effort to make a security culture change. The trend now is to educate the public and the employee base. This new culture where persons have some responsibility for their own safety is the trend going forward.

Behavioral Recognition is already being practiced discreetly at concert venues, amusement parks, and many other resorts. Awareness campaigns, job descriptions, in-service training, and on-boarding enhanced with these techniques will shift the culture from uninvolved victims to interactive groups of people sharing responsibility for their own safety.

This "Human" technology is turning into an industry and a science as we speak. Behavioral Recognition, Security Awareness, and Social Engineering are some of the skills being taught and applied throughout the Security Industry (and the hospitality industry). These fields of expertise, rather than being vague and ambiguous like the See Something campaign, are detailed, advanced, and targeted to certain employee and even visitor groups.

Here are some current examples where Security uses active and passive behavioral recognition to counter potential threats.

- A popular amusement park observes persons entering the venue and refers those with certain behaviors to uniformed police officers. Guests are further examined by plainclothes Security once inside the gates.
- A large mall in the Midwest uses a recognition process to scrutinize its patrons upon entry.
- Many retail chains post persons at the door to greet incoming patrons.
- Many corporations train their employees to recognize the pre-violence indicators associated with workplace violence.
- Did you notice in 2020, when we stopped everyone at the doors and asked them a bunch of questions about the virus, we had no major shootings, no take-over robberies, and hardly any violence to businesses at all. Granted, many businesses were closed, but it is the scrutiny that prevents problems, not the words.

CULTURE CHANGE

The best way to change security culture among non-security employees, is to "deputize" them. Bring them into the fight by showing them what it is we do and what we look for and why. Instead of the new-hire video, make this an ongoing process of learning and awareness. My simplistic notion of this concept goes back to the customer service philosophy of "treat them like guests in your home." When we have a party, we do not worry that our guests will steal our trinkets off the mantle. That is partially because they are trusted friends, but also because they have some "buy-in" to the success of your party. (Let me put this another way.)

You could take a guy that is a habitual car thief and make him a valet attendant. He will not steal those cars because he has some sense of ownership of the job, has personal relations with his bosses and the owners, and wants to do a good job for his employer (well, most of the time).

Suppose there is a romantic scandal at your workplace. The boss seems to be having a nice affair with the Marketing Director. Generally, the clues are put together at lightning speed by the employees until a conclusion is formed. The secretary finds out about the plane tickets to the Bahamas. The security officer sees the two walking to their cars late at night. The wife calls the operator looking for her husband. The director's office door is often locked for long periods of time when the boss is there. The housekeeper finds post-it notes in his trash can with hearts drawn on them. The finance director processes a "business trip" for two to a conference in San Diego. Pretty soon the clues are compiled, and a conclusion is made. Everyone knows.

So why can't we do that with an active shooter? In my opinion, it is not entertaining enough. It also goes against our ability to offend. Wouldn't it be nice if we had all the little tidbits that mean nothing by themselves, but when combined, created probable cause to stop a horrific incident? At least one software company is trying to do just that. They use a database that employees can provide information, without making accusations, that is compiled using artificial intelligence to find commonalities that security can investigate.

Front desk gets a request for a room on a specific floor facing a certain direction. This means nothing by itself. Bellman helps a guest carry several heavy duffel bags and cases to that same room. Guest makes a comment to the bartender that ISIS (a radical Islamic terrorist organization) should be allowed to establish a caliphate because they are just getting even for the history of US aggression toward them. The valet attendant notices the guest is alone and his minivan is full of empty boxes of weapons and ammunition.

None of these clues are significant by themselves but had they been compiled and analyzed before the event, dozens of lives might have been saved on October 1 in Las Vegas, Nevada. This concept is still kind of new and we are still formulating how it works, but meanwhile you can establish a "culture of security" by opening the communication lines within your property so that you might hear of these tidbits. Have you ever heard a rumor at work and thought, "I am always the last to know?" We are so busy with meetings and budgets and scheduling that we often do not spend the time in the lunchroom with our employees or hanging out in a way that we might hear the insignificant things that affect our security.

Suppose you take your valet attendants, bell persons, and front desk staff and put them in a room and ask them, yes, ask them, what type of bad activity have they seen around here. Your socks will be blown clear off. They not only know it's happening, but they know who is doing it and when. So, we have an obvious disconnect. How do we fix that? Instead of asking me or yourself, ask them: What would it take for you to report these activities to me on a daily basis? Again, the answers will blow your hat off. I wager that it will not be monetary gain or even notoriety. It might just be some gratitude. It might be some trust. It might be fixing the refrigerator in the break room. It might be, quit worrying about whether I am stealing paper clips and I will help you focus on the serious stuff. In short, include your employees in the security objective to keep guests safe.

Ownership

Employees from every department need to feel some sense of attachment to the safety and security of the entire building. This is difficult to achieve but it must be done. The way to get it started is from the top down. The big boss and all his/her subordinates need to walk the walk of ownership. Litter on the floor, fire doors propped open, guests taking strollers on the escalators, etc. Employees need to see them addressing these issues and feel a bit of shame, frankly, that the boss beat them to it. Every department needs to have safety meetings and walks to look for problems and correct them. When there is a health inspection or OSHA or Fire Department inspection, all hands should be alerted so they can correct problems before they are noticed. Make all employees aware of inspection discrepancies and explain the consequences of an OSHA notice of violation.

Communication

Besides ownership of the property, is ownership of rules and information. Remember the romance scandal I mentioned before. That could be a sexual harassment situation, and nobody (in my little story) reported it or did anything about it. Again, all employees should feel comfortable mentioning little tidbits to their boss. “By the way, probably means nothing, but Joe is going through a divorce.” And another employee, “Hey Dan, did you know Joe made a comment about how many bullets he could fire in the lobby before someone could stop him?” Sounds obvious, but these are actual statements from actual active shooters that were revealed AFTER they killed people.

As it is hard for employees to reveal these clues because they do not want to get anyone in trouble or, more accurately, they do not want to be labeled as the snitch, make it about gossip and not about getting someone in trouble. I found that I learned a lot more about everything by eating lunch with my employees in the cafeteria. They are eager to gossip and tell stories about other employees in that setting as opposed to walking into your office cold and ratting someone out. Back to the romance scandal, no one is going to report that to anyone officially, but they are just fine talking and laughing about the boss who is not only cheating on his wife, but possibly using company funds for romantic getaways and perhaps sexually harassing his subordinate.

What other ideas for communication have you used successfully? I do not know about your experience, but the hotline and the suggestion box do not work. They tend to be more of a gripe receptacle than a source of useful information. Employees should feel comfortable sharing gossip, ideas, suggestions, and clues with you verbally and openly. Saying you have an open-door policy is also a bunch of balder dash, frankly. Who comes in and says, “Boss, I have something on my mind, so I want to disturb your work and tell you about it." That office is scary, sacred, and not a comfortable place for a subordinate. Instead of waiting for the information to come to you, go to their workplace and visit with them. Talk to them about their family, their hobbies, their interests, and let them know you are open to this kind of talk. I had a director who was a master at this. She was so warm and charming; she would have every employee thinking she was their best friend. About once a month she would come and give me a report about how MY staff was doing and what their gripes and suggestions were. That motivated me to start doing the same.

You, as head security person, do not have to limit this behavior to your department. Imagine talking to housekeepers about their day. How is their job? and so forth. Housekeepers—actually most frontline workers—know way more about your property and its guests than you do. Get to know them and watch the information flow. I got to be friends with a housekeeping supervisor at a hotel where I worked. I soon found out that she knew all the rooms where guests were smoking marijuana. I asked her why she had not reported it. She said her employees felt that security did not care and did nothing about it anyway so why bother. Security actually did care but had trouble identifying which room had the marijuana so they rarely got to stop the smoking. On top of that, the reporting housekeeper never got any results or satisfaction from making the complaint. All we had to do was go back and say, hey we went to that floor but could not narrow it down. She would likely have been able to narrow it down for them. When people make a report (snitch) on someone, they do not consider it snitching because they have "ownership" of the hotel and want it to be clean, safe, and successful. But if they feel that Security is not feeling the same, they will get discouraged and stop communicating.

Going back to a scenario, imagine your world when a housekeeper sees you walking down the hall and says, hey there have been several men going in and out of that room all day long. Ok fine. Then the front desk clerk stops you in the lobby and says, room 916 paid cash and the younger girl with the older occupant looked scared and would not talk. Then the valet attendant reports that he has had several men come and park for an hour or so and then leave. You report this to the police, and they notice the name on the room is a known pimp and they go up and investigate and find a case of human trafficking. It is likely, these bits of information would not have been reported through official channels but building relationships with employees creates those casual channels where the real information lies.

Don't forget to go back to those employees and report that they just saved a young girl's life. Imagine what kind of tips you will get and how many employees they will tell.

Awareness

Once you have the culture of security built into your property, where employees feel ownership, empowerment, and satisfaction from reporting, it is time to tell them what information you want. Each department has a specific set of clues that you want them to observe and report. This is where the See Something Say Something program was lacking—nobody knew what to report. Some suspicious activity is obvious and will get reported, but some needs to be explained, with context, so that employees know WHY they are looking for certain things. I will mention this many times throughout this book, but it bears repeating. Security Awareness and Guest Service overlap so much that they are almost synonymous. This is good news because it makes your job—and theirs—much simpler.

SECURITY AWARENESS

We have all heard the suggestion that "Security Is Everyone's Job." Well, maybe that was "Safety," but it still applies. Whether you have a separate Security Department, it is still a good idea—in fact, it is necessary—that you involve every employee in security. There are several ways to engage the rest of the staff. This becomes a force multiplier for you, increases the number of eyes and hands assisting you, and provides a safer and more efficient operation for the entire business. Most employees will even enjoy the extra work if it is presented properly.

The first step to engaging other departments is to increase awareness. Most non-Security individuals have no idea what Security really does. They may think you are there to spy on them or just to deal with unruly guests. Many are amazed at all of the functions we have in a hospitality environment. Awareness, therefore, starts with an overview of what Security does and the types of things for which we watch. This can be done at a new-hire orientation or a visit during department training. Here are some of the things you can talk about and for which you can develop awareness on your property.

Housekeeping

You do not have to teach housekeepers—or anyone else—to be nosey. Curiosity is inherent in most people, and if anything, it needs to be quelled, not encouraged. Your job, as I mentioned before, is to let them know what things are dangerous or of interest to security. Their guest service, and other skills, will lead them to observe things and behavior.

Housekeepers, or "Guest-Room Attendants" (GRAs), see much more of our guests and their activities than we do. They are (rightly) taught to respect privacy and not go through drawers, belongings, and luggage. We definitely do not want them to do that. After 9/11, we spent a lot of time and resources teaching them how to identify terrorist activity. In retrospect, this was a waste of time, and yielded little. Rather than teach GRAs what is suspicious, we are better served showing them how to report the activity. For example, you do not need to tell an employee to take note of a suitcase with wires coming out of it. Instead, familiarize them with our policies of prohibiting containers of chemicals, machinery, and appliances. Let Security take it from there.

Drugs and Paraphernalia

Many hotels have "look the other way" policy regarding recreational drugs used in the privacy of one's room. Your management needs to decide where to draw the line. A couple of joints or residue of white powder on the desk is different from a brick of white powder with a scale and small baggies. Besides sales, drugs are usually associated with other criminal activity like prostitution, robbery, and organized crime. Do not leave the decision whether to report to the housekeeper or the supervisor. Let them know that Security wants to know about any drug activity and will decide whether to take further action or not. We will review the security side of this equation later in this chapter.

Remember that although housekeepers have a legitimate reason to be in a guest's room, this does not give them cause to open drawers and go through luggage, pants pockets, or anything else that does not involve cleaning of the room. Security has even less cause to go into a guest's room without their permission. The best way to know what your limitations are, is to use the "reasonable person" rule. Is it reasonable to open a guest's room and go through their drawers? Of course not and it is not reasonable. On the other hand, if you heard a strange noise coming from the dresser in a room, you may justify that it was reasonable to find a mouse or other animal in the furniture.

A common search dilemma is for a GRA to find a white powder on the desk, report it to security, and then security's inclination is to see if there are more drugs in the room. This area is so gray that I would advise one of the following: back-out of the room and leave it alone. Take no action. You are not law enforcement and this particular crime—if it is one—does not affect you. If that does not set well with you, then lock the room and call the police. I will tell you now that as I write this, the 9th circuit in California has decided that this would be a bad search, by you or the police, and would throw it out. Police will likely get a warrant if they want to pursue this at all.

Parties

Housekeepers will know when a room has had had more than your registered limit of guests. Call me a "party-pooper" but they are bad news for the hotel. When we have a nightclub, we dedicate Security personnel, bartenders, cleaning staff, and management to protect our guests and our interests. A private party in a room has none of these protections and is not designed for large crowds and alcohol/food service. Some of the issues associated with a party in a room are:

- Unsupervised minors
- Intoxicated minors
- Over-serving or intoxicated adults
- Unsanitary or unsafe food and beverage
- Fire hazards—overcrowding, blocking exit, lack of exits, tampering with fire systems, etc.
- Drug activity, prostitution, other criminal behavior
- Damage to FF & E (Furniture, Fixtures, and Equipment)
- Complaints from neighboring guests

Put yourself in the position of the security manager that breaks up a party in a room and one of the following scenarios takes place: Two 16-year-old girls who were drinking in the room end up going home with one of the adult men in the room and get beaten and raped and dropped off in a nearby park at 3 a.m. Two of the men, not wanting to stop the party, go to the hotel bar and get into a fight before they finish their first drink. Another party guest leaves after being ejected from the hotel and drives his car across the double-yellow line on the main highway, killing himself and a family in a mini-van driving toward the same hotel. Each of these events happened, separately. Who do you think was held responsible for the injuries and deaths in each of these incidents? Always consider this when taking action. Breaking up a party is usually correct, but consequences do not disappear with the party. Make sure intoxicated persons make it through the night safely and that minors, who are now under your responsible supervision, are kept out of trouble. This is discussed in the section dedicated to minors.

Weapons
Many people bring a gun for protection and leave it under the pillow or in a drawer. This should be reported every time. Housekeepers should have clear instructions to vacate the room, report the weapon, and never touch it. Lock the room and inform the guest when they return of your weapons policy. Presumably, you do not allow guns in your hotel, but even if you do, your GRAs do not need to have access to them. Advise the guest of your policy—they either stow it in the safe, their luggage, or somewhere out of reach—or lock it up with security or put it in their car. Possession of a weapon may be suspicious if there are other factors involved, so use your discretion whether the police should come out and investigate. Long rifles, multiple weapons, or unusual weapons should also be reported and acted upon immediately. The only reason one would have a rifle in their room is so that it would not be stolen from the car. Multiple weapons or unusual weapons and large quantities of ammunition and accessories start to raise more suspicion, so discretion is on you. Weapons policy should be considered in your Risk Assessment, Security Plan, Policy Writing.

Prostitution

Most people can tell the difference between a room that has an amorous couple and a room that is being used for prostitution. Though it may seem like it is none of their business, we want our GRAs to report this activity every time. Prostitution means drugs, criminal activity, and human trafficking. (See the section on this later in this chapter.) Many housekeepers and other employees assume that prostitution is part of the hotel business. Make it clear that this is not condoned and must be reported.

Safety Hazards

Many strange activities—besides sex—occur in hotel rooms and when you start seeing it through your guest-room attendants' eyes you will be amazed. I have seen guests rebuilding a motorcycle, storing and mixing chemicals, cooking with microwaves and gas burners, and even setting up hospice care. These situations create dangerous conditions for other guests and you need to know about them. Teach GRAs to report these hazards immediately.

By the way, you may want to remind your staff—and other departments—that we are not in the business of law enforcement and we have no obligation to do so. Our concern is for the safety of our guests and employees and the success of our business. Don't be shy about telling a guest the reason they cannot keep a gas can in a hotel room. It may or may not be illegal, but it is certainly not safe. That cannot and should not be argued. (It is easier to enforce a policy than a law.)

Criminal Activity

I am sure you also have seen drug labs, check printing operations, drug packaging, and other criminal enterprises in your rooms. There are also things that do not quite rise to the level of criminal activity, but you will want to know about them anyway: A stack of credit cards with different names on the desk; a power inverter, soldering iron, or electrical components; pictures of naked children; bloody sheets and towels. Housekeeping knows what is normal and what is not but will not report these things unless you show some interest and provide follow-up with them.

> In 2008, a man became sick in his hotel room in Las Vegas. When Security went to inventory his belongings, they found some guns, silencers, bomb-making documents, and mashed castor beans. The poison Ricin is produced from the mash of castor beans.

Bell Desk—ahhh that bastion of enterprise. Bell persons are not criminals or bad people, but the reality is that they work for tips and are very clever in ways to increase their income. They are not likely to disrupt that income by having you foil one of their games. However, there are some honest ones who will choose company over co-workers and it is those with whom you want to connect.

Bellmen have been known as the middlemen for prostitutes, dances, massages, and everything else since the beginning of time. If they are not involved, they certainly see everything. Their loyalty may depend on whether they are in on the action, but they need to understand the consequences of not reporting prostitution. See the section on prostitution coming up later.

Storage Wars—I have seen the bell desk become a hub of storage activity that endangers the hotel. Homeless, criminals, and other undesirables will take advantage of your free storage service and use it as a transfer point and a free storage while they are out pimping, selling drugs, or begging for money. This is easily solved by limiting storage to hotel guests only and limiting that storage to a few hours depending on the circumstances. There may be exceptions, like a guest attending a wedding at another hotel after checking out, or someone from a business meeting wanting to store their belongings even though they are not a hotel guest. These are exceptions and should not be the rule. Know that the enterprising bell person is in this for tips. Anyone that provides a tip is likely to get whatever they want.

Storing Contraband—The consequences of storing bags for non-guests can be severe. You may be storing a homeless person's bed bug or lice-infested clothing while he goes out to sleep. Or you may be facilitating a drug or other nefarious transaction by drug sellers, pimps, or other criminals who do not want to be stopped by the police when they have whatever is in that bag.

Terrorism—Unless you are in New York, Las Vegas, or most major European cities, you probably don't consider yourself a big target for terrorists. We have seen, however, that criminals of all sorts, including religious and political terrorists, use hotels for planning, staging, and simply sleeping prior to and after a big gig. Vigilance is therefore a requirement for all of us, regardless of our footprint, location, or reputation. The extreme example of storing bags for criminals would be one that we have seen play out in real life over and over again. That is the unattended bag containing explosives or gas or some other lethal agent. Again, even though your hotel may not be a primary target, you may have a target staying in your hotel, eating dinner, or simply passing through on their way to the convention center. The recommendation here is to follow your policies and those recommended here and vigilance will follow. High-risk hotels such as those in New York and Las Vegas go as far as running luggage through airport-style x-ray machines.

Disputes—I cannot tell you how many times a guest has lost their claim ticket and been escorted back into storage to identify their bag. Duhhh. Bell persons are in tip mode, as you recall, and not looking at the big picture. Educate them of the what-ifs, and remind them we have these policies for a reason.

Security may be called for the above scenario of the lost ticket or perhaps a guest complaining that Bell will not accept their bag. There are too many variables to explain here, but remember that bell storage is an amenity, not a Constitutional right. You do not have to accept anyone's bag, but if you are discriminating, you may get in trouble. Instead of limiting the guest, limit the bag. Perhaps it stinks, or has visible bugs, or wires coming out, or perishable food, etc. I do not see any problem with security explaining to the guest that there is a concern about the bag and asking to look in the bag. They did not have to accept and can go elsewhere with it. Otherwise never open someone's property without permission and remember that even with permission, you may be violating their rights if you demand to search it or refuse service.

FRONT DESK

The center of all hotel things is at the front desk. Front desk clerks see everything and know all about their guests. They talk among themselves and are tuned in (better than you) to who is doing what in the hotel. This information can be of great advantage to you or it can be used against the hotel in severe ways.

Identity Theft

We have all heard news stories of persons who went to the front desk and either overheard guest information or were able to fool the clerk into giving it up. Front desk clerks should be told these stories and shown these videos so they can relate to how important their safeguarding of information is. On top of that awareness, set up some simple policies that will keep guest information safe. Simple policies like not verbalizing room numbers, last names, email addresses are vital. A bad guy who gets a guest's last name can do bad things (see Hotel Operator).

Key Theft/Room Entry

Persons who "lost" their key or need a duplicate have to abide by the same policy as everyone else—We need to see ID to issue a room key. What if it is the spouse who is not listed as a guest? Front desk clerks should be taught to ask upon checking in for all names who will be using the room. Do not give clerks the latitude to make a decision to give out a key or to break policy for exceptions. Call security or management. Then you use your internal guidelines to get the guest in their room.

Night Auditor

If your hotel is of the size that your night auditor is the only one staffing the desk after hours (or perhaps is one of two), you need to get them out front and keep them there. I have seen too many cases where a night auditor is in the back doing paperwork while some bad thing or bad people are in the lobby doing their bad thing. It is better to have all clerks out front and visible.

Vertical Security

In hotels where there is no dedicated security personnel, the front desk needs to watch that elevator. A simple “May I help you” to everyone that comes in who is not recognized or does not fit the profile of a guest, will prevent unauthorized people in your hotel. Remind front desk clerks that “ownership” of the hotel includes them keeping out persons who want to do bad things.

There is a growing trend among hotels to staff the lobby elevator bank with someone who will check keys. This is due in part to prostitution, door pushers, robbers, and other undesirable hotel trawlers. If you do not have the staff for this or the hotel is not large enough, use your front desk as the first line of defense for the elevators. Some hotels have upgraded their elevators to require room keys for use. If you can do this and use the front desk as a backup for piggybackers, that would be a good solution.

> Years and years ago, someone left one of those red and white coolers in the parking garage of our hotel. This particular cooler did have wires visible, and some holes cut into it. It looked like an improvised explosive device. We followed our protocol, evacuating and cordoning a certain area of the garage and called the police and fire departments. After about six hours of investigation and lots of gadgets—including a portable X-ray machine and a robot—the cooler was determined to be a failed attempt by someone to make a portable refrigerator. There was a battery and a fan, and that’s about it. It had been apparently abandoned after it inexplicably did not keep beer cold.
>
> The moral of this story was that we did not teach our employees what to look for. Instead, we encouraged them to report suspicious objects and activity. Employees already know what is suspicious but may not know that we want them to bother us with it.

HOTEL OPERATOR

Whether you have a dedicated phone bank (like a reservation center) or your phones are set up so the front desk fields calls, you must have some basic security measures in place.

I have seen so many successful scams, frauds, and major vandalism occur over the phone—yes over the phone from very far away. These are simple ploys, but most employees cannot imagine anything bad happening on the phone, so they are generally in denial. Awareness is the key to keeping guests and property safe. Here are a few examples of actual scams that have occurred over the years.

Credit Card

Bad guy calls the room and pretends to be the front desk manager. "Sir, we had some trouble with the credit card you presented upon check-in. It was declined. This probably an issue on our end, but I need to run it through again. Can you give me that number again—or perhaps you have another card number I can try?"

How do they get the name of the guest? Several ways.

1. Troll social media and find the Griswolds are on their way to Wally World. Call the hotels near Wally World asking for the Griswold room. Finally, you will be connected to him and use the ploy above.
2. Overhear the name at the front desk. "Thank you, Mr. Griswold. Enjoy your stay." Follow them to their room. "What a coincidence, we are on the same floor." Now you have name and room number.
3. (Here is a great one.) Call the employee in Room Service. "Hey this is Chuck in Auditing (or Security or Food Director's office). I need the last four rooms that received deliveries. Names and room numbers." Then Chuck calls the rooms and does the same credit card ploy. "Sir, your credit card for that breakfast did not go through. May I re-run it please?" Usually, no suspicion because who else would know he ordered breakfast?

Vandalism

I am sure you heard of the pranksters that called rooms in hotels years ago and convinced the guests they needed to throw televisions out the windows, break open fire sprinklers, and smash balcony glass doors. This really happened and people really fell for it. Hundreds of thousands of dollars in damages were racked up with little recourse to recover the money. I do not know of a remedy against this kind of mindset.

Long Distance Call

This scam, a bit outdated now, was perpetrated mostly on unsuspecting employees. The caller would get to an obscure department like Purchasing or Housekeeping and say something like, "I have been transferred all around this %$#@& hotel and everyone keeps screwing it up. I am trying to get to your Corporate office to make a reservation." The employee answering the phone does not know that number, so the caller gives them the number with the area code, which is an overseas number. Less important than the amount of the phone call was what was discussed on the call. It could be a criminal enterprise successfully hiding their tracks.

Purchasing Scam

Another phone scam perpetrated on employees is where the caller poses as a vendor who sells printer cartridges, for example. Rather than going through Purchasing as your company requires, they call the department directly and say, "We are your new office equipment supplier and part of our white glove service is to call you periodically and make sure you have what you need. How many toner cartridges…" and so on. The department may or may not receive the merchandise but Purchasing will definitely receive the invoice that the employee authorized and will have to pay it.

> One more:
>
> Bad guy calls catering manager and wants to book an event. Food, space, and amenities it gets up to about $5,000 and the manager sees her bonus dancing before her eyes during the call. This is a good day. She informs the "client" of a 20% deposit to hold the space. No problem, says the caller, except that her Corporate folks gave her a $3,000 check to secure the event and buy party supplies and such. "If I send you this $3000 check, can you send me back a check for the difference so I can buy those supplies?" Of course, what harm could there be in that? What the caller is counting on is that your accounts payable department is way more efficient than the accounts receivables. That check for $2,000 will go out ASAP because it is a special deal requested by the department head. By the time the AR folks realize that the $3,000 check is bad, it will be too late.
>
> *Note: if you have seen those jobs advertised where you work from home opening envelopes and re-sending them to a different address, this is where that comes from.*

Solutions and Policies—Most of our internal controls can prevent all or most of these scams. I recommend doing the following if you have not already:

1. Require a name and room number when transferring a call to a room.
2. Do not allow guests to call from one room to another (go through the operator).
3. Tell guests in collateral and verbally that you will never ask them for personal information over the phone.
4. Present these examples to employees and remind them that blind phone calls are just like Phishing emails and should be scrutinized.
5. Record your operators' phone calls where the law allows it.

BEHAVIORAL RECOGNITION

There are many training programs available to teach your security staff how to recognize suspicious behavior. While they focus on one type of activity, such as suicide bombers, active shooters, and other violent behavior, we can use the basics of these programs to identify just about anyone who might threaten our assets.

Profiling has gotten a bad name as some lawyers and others misconstrued it as discriminating based on protected classes, such as race. Discriminating based on physical characteristics is not what behavioral recognition is about. The only time we would use physical characteristics to suspect someone is if he or she matched a description of a known criminal or from a group of potential offenders. For example, if you were trying to challenge any member of a Hispanic gang from entering your facility due to a Hispanic wedding taking place, you would use "Hispanic males" as one of the identifiers of those whom you stopped. Note that I said "one identifier" because not all Hispanic males are gang members. The public learned shortly after 9/11 that not all terrorists are of Middle Eastern descent. Not all Middle Easterners are Muslims and not all Muslims are terrorists. Therefore, we concentrate more on behavior than on appearance, but we do not exclude appearance completely.

The following steps need to be implemented outside the building whenever possible. Once a perpetrator gets in the building, it is much more difficult to get him or her out. In the case of a random shooter or bomber, all he or she wants is to be inside, so it may be too late. This applies to nightclubs, amusement parks, etc.

Step One—Objective

The first step is to define the activity we are looking to prevent. In a hospitality environment, it may be a suicide bomber, active shooter, violent employee, or other unwanted persons like gang members, drug dealers, and pedophiles. Of course, your answer is that you want no one from that list on your property. That is fine as long as your spotters know what their objective is.

Step Two—Observe

Next is to observe persons approaching the property. Because we are trying to prevent so many types of behavior that are dissimilar, it is simpler to find the behavior that is out of place. After watching guests for a few hours, you build a "profile" of what a hotel guest or nightclub visitor looks like. Then you look for the ones who do not match that profile. It may be a little different from hotel to hotel, but it may include persons who arrive by bus or walk to the property; persons with no luggage; persons traveling alone; young males alone; persons not talking or texting on a phone; persons wearing different clothing, such as heavy jackets, caps, sunglasses at night; and so on. Note that this is where some people get into trouble. None of the activities from this list constitutes violent or criminal behavior. Combined with other characteristics, they may exhibit behavior worth watching: looking around at cameras and security elements, avoiding eye contact, fixed stare or gaze, and being nervous or agitated.

Step Three—Second Look

This is what I call the second opinion or inside layer. Ideally, the outside officer sees a person with a heavy coat, walking alone, with a fixed stare, heading toward the front doors. She radios it into the officer watching the lobby or a dispatcher who can track the person on camera. The second officer makes the same observations and either confirms it or discounts it with new information. This officer or dispatcher makes the call to challenge the subject.

Step Four—Challenge

Finally, the challenge. In the hospitality environment, we have to balance the elements of our mission in all situations, especially this one. We want to know who this person is and what he is doing, but we also want to make our guests feel welcome and comfortable. Therefore, while we consider this a "challenge" of the subject's attention, those around us should see this as simple guest service. This is where training meets professionalism and attitude. One—and only one—officer should approach the person outside of the entrance and simply ask some service-related question. "Can I help you find something?" A regular guest will answer quite normally. "I am looking for my family" or "Yes. Where is the restroom?"

This gives the officer a chance to do some close-up analysis of the subject. Eye contact, smile, nervousness, and other facial and body language will decide whether more questions should be asked. Follow up on the answer to the first question or ask other questions to find his intent in the building. Honest persons will provide quick, helpful answers. Persons who are lying tend to have slow, broken answers, with lots of mistakes in grammar and content. This is because they are processing the story they memorized and repeating it back. This also causes heightened arousal, which can lead to sweating, facial itches, fake yawning or chewing, and agitation. At some point, the subject either will convince you he is a legitimate guest, or he is uncooperative and that is the point you ask him to leave. The bottom line here is that this is private property and if you are not a guest, we have no use for you, so have a nice day. Of course, we use courtesy and firmness to avoid offending anyone. I treat everyone as if he is the son of my boss, who will be reporting to her on my actions.

Avoid lying when approaching suspicious persons. I have seen officers tell the subject that he looks like someone in a wanted photo or someone they kicked out before. You do not need a reason for stopping and talking to a guest. If it is done in a friendly way, a legitimate guest will not have a problem with it. You can always tell the truth—tell them they looked suspicious wearing a big jacket in a warm building or they were sweating and pale so you were concerned for their health.

While traveling in a major U.S. city with my teenage son, we entered a famous office building looking for the observation platform on the top floor. As soon as we walked in the main doors, two plainclothes security officers immediately approached us from opposite sides of the lobby. One asked me if he could help me. I was dressed as a tourist, so it was obvious I was not a businessman and had entered the wrong doors. I told him I was looking for the entrance to the platform elevators and he explained I was in the tenant entrance and directed me to the proper place to go. I was not offended or embarrassed and later told my son they probably had Uzis under their jackets for the real bad guys. They were well trained in customer service, behavioral recognition, and probably combat.

Security officers need to be better trained and use more discretion than "guards" who do not know better.

If we could put metal detectors and x-ray machines at our front doors, we would not have to think of clever ways to predict behavior. Unfortunately, this is not conducive to our hospitality environment. Instead, your detectors are the employees who staff the entrances of your facility. In a hotel, that would include Parking Attendants, Valet, Bell Desk, Front Desk, Landscapers, Maintenance, and Housekeeping. These employees should be exposed to a behavioral recognition class that provides the awareness needed to identify unusual or aggressive behavior and the steps of notification.

These employees should be watching out for physical and behavioral signs mentioned previously. It is also advisable to provide photos or BOLOs (Be on the Lookout) to these departments. Not only does this make them aware of known criminals in the area, but also it gets them accustomed to watching people's faces.

When employees observe suspicious behavior or see a suspected bad guy, they should have a system in place for contacting security. This can be a simple phone call, a silent alarm that activates door cameras, or even hand signals to other employees. This information, one way or another, needs to get to security or the appropriate person who will challenge the person.

Security officers have been observing mannerisms and appearance, comparing them to the environment, as long as anyone can remember. It has been a simple and effective way for any person to notice someone that is out of place or doing something that is not appropriate at the current time and place. This technique would go along unchallenged, unnoticed, and taken for granted until the 1980s when it became a racial issue. Police officers, who were not necessarily trained to recognize behavior in this manner, but used their experience and instincts to identify potential bad guys were labeled racists because in most cases, they were white and the suspects were black. The technique at that time became known as racial profiling and took on a negative context to which most of us steered clear.

Since that time, police officers have been formally trained to focus on a person's behavior rather than the color of their skin. In our profession, we must also train our security officers to recognize a person's behavior and its association with the time and place before we call it suspicious. In my opinion, it is not behavioral recognition that requires special training, it is the abuse of this type of recognition that we have to teach our people to avoid. I further believe that because most people can recognize suspicious behavior, we do not have to train them to use it, but to put it in a context that will not allow bias.

We can teach our security officers and most of our other employees to be a part of the behavioral recognition process that we will use on our property. As I mentioned before, behavioral recognition is simply observing someone's actions and their appearance and putting it in the context of the current time and location to see if anything stands out as unusual. It is important to note that by appearance, I am not referring to race or ethnicity or any of the other protected classes that could be construed as discriminatory. I also want to caution that nothing I am talking about refers to violating anyone's civil or constitutional rights. As we go forward, I will distinguish between what is legal and what is not.

Appearance in the context of behavioral recognition is simply matching the way a person looks with the current environment. For example, a man who walks into a Phoenix hotel in July wearing a heavy jacket down to his knees, does not match the current environment. This is not to say that wearing a jacket in hot weather is against the law or even a problem for us. But it is unusual, and it gives us our first indicator that we want to understand before allowing the man to stay. Same goes for a man who we know is staying in our hotel, but who has brought ten pieces of luggage yesterday and ten more today. Maybe he got kicked out of his house. Maybe he is a salesman going to the nearby shower curtain expo. Maybe he is a killer who wants to use your balcony as a perch.

Our objective then, is to train all of our employees to greet everyone and when they see the guy with a trench coat or the ten pieces of luggage, we mentally flag him to be approached. The person who makes this approach may be security, or a manager or whomever has some advanced training. That person, who has had more training and behavioral recognition and experience working at the hotel and the maturity not to jump to conclusions, would approach the suspicious person. This should not be a contentious confrontation but a continuation of our guest service. You may choose to use more direct questions, such as where are you going? What can I do for you? And even, why do you have so many pieces of luggage?

During his first round of questioning, we make observations of the subject's behavior as he answers questions. Someone who evades questions, acts nervously, and is not sure how to answer, should raise even more red flags. You will decide by policy how to proceed with this type of person. Perhaps a manager gets involved and makes a decision. Perhaps security has the authority to investigate further and the man if necessary. You may also wish to simply observe the person—after telling him you are finished and thanking him for the trouble—and see if you can find any more relevant observations.

Many organizations use the first part of this process to enhance their guest service. I have been to many businesses where the first priority is to acknowledge the guest as mentioned above. We seem to have gotten good at this step, but the remaining steps have been forgotten or neglected.

I strongly recommend using behavioral recognition at the entrances, at elevator banks, in the hallways of your hotel, and anywhere that people are encountered.

Getting employees involved in some of the layers of security makes your property safer and multiplies this human layer of security.

SOCIAL ENGINEERING

Social engineering is a somewhat new name for an old trick—the confidence trick. Grifters and others have been using this method of theft for decades. It is called social engineering or a confidence trick because the con artist uses social interactions to gain information or property unlawfully or against the person's knowledge. In a hotel there are several ways to do this, and it is important to familiarize our employees with these scams for the safety of our guests, their property, and their information.

Front Desk

John goes to the front desk and asks the clerk if they received a package in his name that his company has been forwarding all over the country to catch up to him and he really needs it for his next sales meeting and blah blah blah. While the clerk steps away to check for his package, John listens in to the transaction taking place at the counter next to him. The Smith Family is checking in from out of town. They are heading to the amusement park tomorrow and cannot wait to get settled in with all their stuff. John overhears the family name, the name of each adult, their address, email, and maybe a credit card number. But he won't need that. He is just a thief.

The next morning, John comes back to the front desk. There is a new shift of clerks who does not know him and quite a line of people checking in and out. He is nicely dressed but in a panic, as he is late for a meeting and has left his briefcase with his wallet and room key in the room. "Sir, I cannot give you a duplicate key without seeing your ID." "Listen lady, perhaps I need to see your manager! I just told you it is locked in the room! You must have a policy to deal with these types of situations." The manager comes out and John is now the nicest guy in the world. "Look, if I miss this meeting, I lose this account, and my wife, who I brought along will be pissed and it will ruin our entire trip. I can give you my name, her name, our address…I can even give you our email…" Two minutes later he is in the room.

In 2008, a man was stalking a famous female sportscaster and was able to convince hotel employees to provide her room number and dates of her hotel stay. The man successfully recorded video of the woman in her room naked using a reverse peephole camera. He recorded two videos of her, posting one online which went viral. The man was arrested months later, and the woman sued him and the hotel for 75 million dollars. Ultimately the jury awarded the woman $ 55 million explaining that the hotel was 51% responsible and the stalker 49%. This is an example of social engineering and one reason why front desk clerks do not give out the room number verbally to guests.

In the early 2000s a new prank started appearing in the news. It turned out to be not just malicious but felonious and that ended up costing hotels and restaurants tens of thousands of dollars. The prank though it had several variations went something like this: The caller would somehow get through to a room on the telephone and tell the occupant that he was a member of hotel management. In a panicking voice the caller would say that there was a gas leak or some other type of eminent threat that required immediate action by the victim. The caller was able to convince several people to bust sprinkler heads, throw TVs out of windows, and otherwise cause remarkable damage. The amazing thing—besides being able to find people in hotels that gullible—was that the suspects were untraceable and therefore unable to be prosecuted. The police were hesitant to charge the persons doing the damage because malicious intent could not be proved. So in most cases no charges were filed and the hotels—or their insurance companies had to foot the bill.

The Catering Department (or reservations or the restaurant) receives a call from a potential customer that wants to rent some meeting space. Of course. We require a deposit so if you send me a check for $1,500, we will set everything up for you. The caller says perfect. But I need a favor. My boss will only write one check for this meeting and I still have to buy some decorations, awards, and so forth. If I send you a check for $2,000 can you send me back a check for $500? Well, I don't want to get scammed so I will wait until I receive the check and then I will send it. Of course.

By the time the bank tells the hotel that the check is no good, the $500 has already been mailed out. This is a common transaction and takes unsuspecting companies every day. In fact, you may have seen certain job opportunities where the task is to receive mail at your house and forward it. This is one of the uses for that scam.

Room Service receives a call from "Cathy" in Auditing. Cathy says she is doing a real-time audit of room service charges. She needs the name and room numbers of the last three room service orders made with a credit card. "Now it's against policy to give me the credit card number over the phone, so just tell me the last four digits of each credit card." The Room Service clerk finds this a bit odd, but after all, what harm could come from giving out a partial credit card number? And besides, we are slammed now and it's just like auditing to pull this during the breakfast rush, so he complies just to get Cathy off his back.

Armed with her new information, Cathy calls the operator and asks for the first name on her list along with the room number because we have a policy that requires you to have both pieces of information before we connect you to a room. The guest, who is certainly in the room awaiting his eggs and bacon, answers and Cathy tells him that during the rush to take orders this morning, we must have gotten your credit card number wrong because it did not go through. Cathy further states, "You don't know me, I could be anyone trying to get your card number so here are the last four numbers on your card." The guest complies happily, thinking this hotel really protects its guests well.

Cathy is actually in a room called a phone bank located in eastern Russia where she is paid a commission for each good credit card number she obtains. This card number along with hundreds of others will be sold in bulk to other criminals who will either make their own credit cards or use it online a year later. By that time, our guest has no recollection of this transaction and will have made dozens more. By the time he realizes he has been defrauded, it will be too late to do anything.

Certainly, the credit card company will reimburse the card owner for most of his losses. They will use the purchase patterns of the bad guys to try to thwart these transactions in the future, but nobody, and I mean nobody is going to investigate the crime, go to Russia and file a civil suit, make a claim against the credit company, or do anything substantial to solve this crime.

There is only one way to prevent any of these scams—tightened procedures. If each of the employees in the preceding scenarios had followed simple procedures, the scammer would have been defeated. Just like when we hear shots fired, we go into denial, thinking, what are the chances I am getting scammed? If you do not have procedures for giving out information on the phone or in person, establish them now and make sure they are enforced.

Some call these types of scams "social engineering" and the techniques have been used to steal our defense secrets, and to steal millions from corporations and individuals. Just like our guests who slip into vacation mode, our employees also become lax when dealing with people at work. They would never give out information to a telemarketer at home, yet their guard drops at work. Plus, we are taught to bend over backward to make a situation work out for our guests.

There is a difference in courtesy in appeasement. Politely telling a guest No may be the only option no matter how persistent they are. For example, the catering manager may want the sale from the caller who wants to send a bloated check, so they become complacent with procedures. The risk is worth the reward to them. But if your procedures require all checks to go through accounting, there is no way that scam is going to get past your accounts payable department. Same goes with the alleged "audit" occurring over the phone. If the call-taker simply says, you need to come down here or talk to my manager, then game is over. But everyone wants to help. We want to steer that helpful attitude into one of communication and reporting.

Consider audits that test the employees for their tight lips. Have accounting or whomever call the room service clerk and ask for credit card numbers. They pass the audit when they refuse to give out the information and vice versa.

WORKPLACE VIOLENCE

Workplace violence is one of the biggest issues facing the business world today. The hospitality industry is not immune from criminal acts that range from bullying to mass murder. Many of the incidents that have occurred over the past 40 years have taught us how to prevent them. All we need is a strong prevention program. Before we outline that program, we will look at the history and types of workplace violence.

OSHA defines workplace violence as any physical assault, threatening behavior, or verbal abuse occurring in the work setting. This includes a lot of different violence, so it is further divided into four types.

Type I—Criminal Acts

Violence resulting from criminal acts committed by strangers is by far the most common. In this type, the perpetrator is not an employee and has no relationship with the business or the employees except through the criminal act itself. This type includes robbery and even terrorism. As you might guess, taxi drivers are the most common victims of Type I violence. This chapter will not review prevention methods for robbery and other Type I violence as it was discussed as part of the Security Plan in Chapter 2.

Type II—Customer/Client/Patient Violence

Type II violence includes any type of violence where there is some sort of business relationship between the perpetrator and the company. Patients who commit violence in hospitals are the most common Type II violence. Mental patients assaulting doctors, disgruntled customers attacking salespersons, and even a guest attacking a prostitute in a brothel would be examples of Type II violence. This type is not discussed in this chapter, as violence from outsiders (guests) should be addressed as part of our Security Plan and there is no way to prevent it using the techniques to be discussed here.

Type III—Worker-on-Worker Violence

This type of violence is the one we most commonly associate with workplace violence. The term "Going Postal" (discussed later) derives from this type and includes any type of violence between current employees. It also relates to violence caused by a former employee or even a contractor or vendor. This type of violence is preventable because we know or have known the employee and we have some control over his or her behavior. We at least have the ability to monitor the behavior before it becomes violent.

Type IV—Violence Stemming from a Personal Relationship

Type IV is another type commonly associated with our image of workplace violence. In this type, the perpetrator is an employee, a former employee, or is involved with an employee in a personal relationship. Because we may or may not know the aggressor in this type of violence, we need to identify the victim, who is our employee. This is not so difficult, and we will discuss this here as well.

History

In 1986, a postal worker named "Crazy Pat" walked into work in Edmund, Oklahoma, shot 14 co-workers, and then shot himself. In a few minutes, Pat had changed our view of workplace violence forever. He had been described as odd and a loner and had been involved in several confrontations with other employees. In fact, management was preparing to fire him for that behavior, but they never got the chance.

There were several similar shootings at postal facilities (and other businesses) up until 1993. In retrospect, the term "Going Postal" was earned by the United States Postal Service (USPS), which had a work environment that was ripe for violence. In the 1980s, the USPS employed over 900,000, so statistically it was bound to have a large percentage of workplace incidents. It also had the largest and one of the most powerful unions in the world up against a huge government bureaucracy, which made it easy for individuals to feel insignificant. As new companies like FedEx and UPS emerged, it became apparent that the post office had competition for the first time ever.

As a result, this bureaucracy started focusing on productivity and timelines more than ever and worker stress rose sharply. From 1986 to 1993, 1 in 12 postal workers had filed a grievance against management, which likely raised the stress levels even more. These grievances and other employee issues and morale were secondary to the timely delivery of mail. Right about that time, email changed everything.

Meanwhile, other companies had their own issues with Type III violence. Several current and former workers committed more mass killings. Background checks, which were previously reserved for security officers, money handlers, and managers, had to be completed on employees of all disciplines in any size company.

In 1993, after five more mass murders at postal facilities, management started to take notice. The first solution was to establish a toll-free hotline for postal employees to report management abuse and other unfavorable work conditions. It was shut down a short time later because there were too many calls. Later that year, a new position called Workplace

Environment Analyst was created to focus on the prevention of workplace violence. This may have had some limited success because there were no more mass shootings at postal facilities for several years.

In 1998, the U.S. Postmaster created the Commission on a Safe and Secure Workplace. This study did not receive much attention because "Going Postal" had kind of left the post office, but it created some prevention methods that are still in use today. Those will be discussed later.

Meanwhile, the late 1990s had several more mass workplace shooters. Many criminologists attempted to create a profile of the potential workplace killer but were unsuccessful. The physical characteristics of these murderers were of all races, ages, nationalities, and both genders. Some were blue collar, and some were professionals. We even saw teenagers get into the action at a Jonesboro, Arkansas, middle school and later at Columbine High School in Colorado.

As workplace homicide entered the 21st century, it finally became apparent that there were two things that contributed to this type of violence: difficulty dealing with anger, and the "end of the line" feeling following a termination. But most important, more than 80% of these killers left visible signs of their violent behavior—and not one of them "just snapped."

Conclusions

The 40 years of history lead us to some conclusions. Most attackers had no criminal record, but they almost all had poor job performance. As mentioned previously, they crossed all economic and social levels, were either current or former employees, and were of almost every race and gender. About half of them committed suicide. Almost all of them were motivated by anger, usually at the supervisor, and either had been terminated or were facing termination. About half of the murders occurred the same day as the termination and the other half occurred up to a year later. One postal worker waited three years to kill her co-workers. Very few had undergone a background check, or their violent backgrounds were ignored.

Two of these factors are screaming for attention. One is the previously violent behavior, as noted by warning signs. Two, is the pending termination. We can deal with these two tangible subjects. Before we extrapolate those into some prevention methods, let us have a quick look at anger.

Anger

You may have learned in your college psychology class that there are two personality types: A and B. Anger is normal to each of them, and that anger can turn to violence in some people.

Type B personalities tend to be very passive. As they get angry, frustration builds until it turns to aggression. That aggression can turn to physical violence in some persons. This is not to say that every type B personality becomes violent; it only shows us how they could become violent. I like to think of a character like Darth Vader in the movie *Star Wars.* He started out as a happy, passive child, until his mother was murdered. He started displaying signs of aggression and violence that some noticed, and some did not. His anger built up to the point where he turned to the "dark side" and became a mass murderer. This type of person faced with losing his job might appear to "snap."

Type A people are generally aggressive in their daily routine. The angry ones tend to be mean and are the ones we consider bullies. They have to show their superiority by making others feel inferior. Imagine someone like that being fired from his or her job. "You are firing me? I will show you who's boss." The embarrassment and loss of control become overwhelming to them and they decide to end everyone's life including their own.

These personality descriptions are very general and overly simple. We all understand that human emotions are very complicated, and it takes years of education to get a grasp of them. For our purposes of developing a prevention module, the simplified version should suffice.

WORKPLACE VIOLENCE POLICY

The first step to prevention of workplace violence is to establish a policy. You may already have one, but if you do not, get some help in writing it. It is the Human Resources Department's job to write employee policies. Your labor lawyer or general counsel may have some input and there are plenty of samples on the Internet.

The policy should have three elements. First is your company's definition of workplace violence. The policy we started with might suffice, but make sure it includes threats, bullying, harassment, and intimidation in addition to physical violence. Second, it should include the duties of management and the duties of employees. For example, all employees have a duty to report workplace violence even if they are not sure whether it actually happened. Management has a responsibility to thoroughly investigate all reports and to report violence to HR and Security. Third, it should outline consequences. Define what will happen to those found in violation of the policy and what will happen to those who make false reports.

Make sure the policy includes the company name. It is important to make the company the victim rather than the employee. This will make some perpetrators realize that if they attack an employee, they are attacking the entire organization. This is a subtle scare tactic to potential offenders, and it shows your employees, and any potential victim of such behavior, that you have their backs. Avoid using phrases like "zero tolerance" and defining specific penalties for violations. Part of the prevention process is a negotiation with a potential killer, and we need to leave some wiggle room to do that. Also, avoid promises of confidentiality. You cannot guarantee that a witness or victim will remain anonymous. You may need them in court or a police report.

Developing the Program

There are several components involved in developing the program. First, review your company's pre-employment screening. Work history should be thoroughly checked. Interview questions should be designed to provoke responses that will reveal violent tendencies. Consider using a second interviewer or a team interview to get a valuable second opinion of personality. Always drug screen every new hire. Also, consider running contractors and vendors through a similar process.

According to the State of Wisconsin Department of Administration, “firings are the cause of most violent, rampage attacks in the workplace.” Actually, that is like saying guns are the cause of most murders. Terminations are the *motive* for most of these mass murders. Knowing that, we can train our supervisors and managers, in all departments, how to discipline and terminate employees. It is possible to avoid that “end of line” feeling when firing someone, but it takes some tact and it takes more time. Supervisors should also be taught how to properly discipline employees so that it is a positive coaching experience rather than one that will leave an employee angry and vindictive.

Managers and supervisors also can be taught how to identify the behaviors that indicate a tendency toward violence. Employees who make threats or react irrationally to trivial matters should be identified and the situation resolved as soon as possible. Employees usually know the signs before anyone else and can be extra eyes and ears to future problems.

If your company does not have an employee assistance program, you should look into getting one. If you have one, make it more than a brochure in the Benefits office. This is a valuable employee benefit that can be used early in the escalation of violence. Use it to get help for employees before they become a violent problem. Sometimes this program and others can be used in lieu of termination. If you have an employee with an anger management issue, order him or her to seek counseling as a condition of employment. This defers their anger back to themselves. If they drop the program, it is on them and not the company. Other negotiating can take place to avoid violence. If you want to get rid of someone who you fear is going to be violent, why not buy them off? Maybe you allow them to resign, or you promise not to contest their unemployment benefits, or even give them a severance. A few thousand bucks to have someone leave with a smile will go much farther for your peace of mind. I did not believe this until I tried it.

We had an employee who was a loner. He did his work for the most part, but was mediocre at best and did not get along with others. One day, his co-workers teased him about some less-than-great work he did. His response was: “One of these days, I am going to come back here and mow all of you down with my AK-47.” This was a union employee and if we had fired him, it definitely would have come back as a grievance, that he was just kidding, or something similar. Instead, we got together with his department head, the union leader, and our labor counsel. We all agreed we were scared to have him on the property and equally worried that he might actually come back and make good on his threat. We got the union representative to buy in to a deal where the employee resigns and collects unemployment and all his accrued vacation time. Nothing would go into his file because he was resigning. I cannot express the relief on everyone’s mind when that employee shook everyone’s hand as he left and bragged about all the fishing he would be doing. It cost us about $5,000 and was worth every penny, especially because we would have spent that anyway on a grievance and labor board inquisition. He left without an “end of the line feeling.” He had hope and optimism.

Another useful tool is the exit interview. A good exit interview can be used just as the hiring interview to identify violent emotions. Ask questions to find out about his state of mind regarding revenge, anger, and whether he has any hope for future jobs, where to live, income, bills, etc. This is not necessary for every employee and not everyone will do it, but most angry people want to vent to someone. The venting alone may be enough to avoid a problem later.

Related Policies

Besides having a workplace violence policy, there are other policies important in preventing it. Drug use and possession, in some cases, go hand in hand with violence, theft, and other misconduct. It has no business in the workplace and your policy should reflect that. In recent years, companies have stopped doing pre-employment drug tests. Because of the formerly illegal drugs that are now legal, and opioids which are easily justified as medically necessary, along with the fact that the testing did little to “weed” out bad employees, the decision made sense. On top of that, OSHA came out with a vague statement that drug testing discouraged employees from reporting illnesses and accidents. So much for that. Cause testing is still a good option. That is discussed in the Investigations chapter.

Weapons should be prohibited on property. Some conservative states, in efforts to protect gun rights, have legislated rights of individuals to carry guns in their cars, whether the employers permitted it or not. Whatever the laws in your state, you do not have to allow weapons on your property. If you are in a right-to-carry state, provide a safe place and method for employees to secure their weapons at work so they are not stolen from their cars.

Anonymous tip lines have been addressed in a couple of places in this book. Workplace violence prevention is a perfect reason to have an employee tip line. If someone is worried for their safety or does not want to be directly involved, they should have a mode of communicating directly with management. One way to do this is setting up a voicemail box that is only accessible by Security or HR.

Training Program

Once we have our policies in place, it is time to train everyone. Training needs to start at the top. Executives are trained first to get their buy-in and support. Supervisors and managers need training in leadership, prevention, and awareness. Leadership training includes proper counseling techniques, terminations and layoffs, hiring and interviewing, etc. Prevention includes how to intervene in a violent situation, de-escalating a violent employee, and avoiding mistakes that create a violent or uncomfortable atmosphere. Awareness training is most of the information contained in this section of the book. All employees should know what causes violent behavior, how to recognize it, and how to report it.

Conflict resolution training is not only good for guest services and handling complaints, but supervisors and co-workers can use it to maintain peace in the work area. Employee assistance programs should be made clear to every employee so supervisors and co-workers can see the value in this free service. Active shooter training and response to other emergencies should be given to all employees so they know what to do in the event there is a dangerous episode while at work. Finally, communication should be included in this training. Where do employees go to report violence? What type of violence do they report? Who has to be notified? What if there is an incident off-duty? As I mentioned before, *document* all training.

Threat Management Team (TMT)

Also called Threat Assessment Teams (TATs), this is one of the solutions I mentioned earlier that was developed by the Postal Commission. The TMT or TAT is made up of HR, Legal, Safety, Security, Employee Assistance Program (EAP), and even medical professionals from your company or from outside. When a report of violence or a potentially violent person is identified, this team is assembled to review the case. They can come up with alternatives to termination and a comprehensive course of action that is in everyone's interest. Some of their options are to recommend medical or psychological treatment, to require a fit-for-duty evaluation, reassignment of the offender, anger management training, and many other clever ideas.

This team manages the prevention program to keep it current by making changes. In the event of a major violent incident, this team would communicate with staff, the media, and police to control information going out.

Domestic Violence

Most of the prevention methods we discussed previously are related to Type III Workplace Violence—the disgruntled employee. Type IV, as you recall, was violence from a domestic situation involving an employee. In that type of violence, we often do not know the aggressor and certainly do not have any control over him, so our first step is to identify the victim. First, here is a very brief history.

Domestic violence in the workplace does not always get the same headlines because there is generally only one victim. But, as we all know, everyone in the workplace can be traumatized or even injured or killed because of this type of violence. Over the past 40+ years, society has taken a very strong stand against domestic violence. Restraining orders are handled as a matter of routine, and friends, neighbors, and relatives of victims tend to be more aware and more willing to assist someone who is being abused. Unfortunately for us, the aggressor has learned that it is much easier to abuse the victim at work than at home. There are no family members, dogs, or alarm systems to protect the victim and the aggressor knows right where to find her.

Here are some statistics: 74% of domestic violence victims are harassed at work, 64% of domestic violence victims report that their job was adversely affected by their attacker, 83% of EAP referrals are for domestic violence, and 15% of women who die on the job are killed by their abuser.

Relating back to our risk assessment in Chapter 1, we need to do something to mitigate this type of violence. Our first step is to identify the victim (because we do not know the aggressor in most cases). Most people have been exposed to domestic violence enough to know that a victim experiences unexplained bruises, absences, and anxiety. Their lack of concentration or disruptive phone calls and visits affect their job performance. The best way to identify a victim is to just ask them. What? HR always says we cannot ask about someone's personal life. Of course you can. If there is something affecting a person's job performance, you can certainly ask what it is.

Once we identify a victim, we need to help them help themselves. As mentioned before, this is not only for them but also to protect our other employees. We can help someone get a restraining order by walking her through the process, going with her to court, or giving her work time to go to court. If a regular restraining order does not suffice, some states allow companies to get a restraining order. This takes the heat off the employee and puts it on you.

Other options include the EAP or other counseling, increased security such as escorts to the vehicle, panic alarms, and special parking arrangements. HR can consider temporary reassignment of the victim to get her out of public areas or even relocation to another property.

As a last resort, there is termination. That's right: termination. If you have a victim who is being beaten at home, receiving threats that her boyfriend will kill her at work, and she is doing nothing to help you prevent the problem, you may have no other choice but to terminate her. This is better than putting all of your other employees in danger and disrupting the business. Tell a victim that this is an option, and that may solve the entire problem.

Conclusion

You have many eyes watching the way you deal with workplace violence: The Big Man and all of the previous victims of bad management; OSHA; National Labor Relations Board; your State Labor agencies; the police; Civil Court; the Building and Fire codes; your community; your boss; and your conscience. This is one area where there is plenty of foreseeability so your career and even the business may not survive a significant incidence of violence that could have been prevented. Take some time on this one and do it right. Remember that your guests can become victims of workplace and domestic violence.

VALET PARKING

Valet parking is often overlooked from a security standpoint because it is an amenity that the hotel relies upon to establish its posture. Valet is often the first impression given to the guest yet may be the one to which is given the least attention. You likely did not come here to learn how to run a valet department, but many security directors are given the Valet responsibility. This begs the question of who is going to deal with reports of damage, missing vehicles, drunk drivers, and even drunk employees?

Here are some of the claims and incidents you can expect to see in Valet and how to mitigate them. By the way, there are thousands of valet operations in this world and there is nothing you will encounter that has not happened elsewhere. So playing ignorant with the anticipation of these claims is futile. It is better to learn from others' mistakes and calamities than risk the chance that they will not happen.

Most common of all claims in valet is vehicle damage. There are so many factors in a damage claim that we need to cover all the bases. First, in my experience, about half of the claims you will get will not have even happened on your property. The damage may be pre-existing, or it may have occurred after they have left. Second, the employee may have damaged the car and did not report it or did not know he damaged it. Valet drivers are experienced just because of their job, so damaging a car is unlikely, though with so many cars, the odds are that it will happen often enough.

The final scenario is that the car gets damaged by a third party while it is in your custody. The industry has ways of protecting itself from these claims, or at least narrowing down the fault of the damage. Here are some measures you should consider for your Valet department, whether you run it or not.

Video Cameras

Place video cameras at the point—or entrance—where vehicles enter the concourse. A minimum of one camera on each side of the vehicle at vehicle height will save you lots of time and money. If possible, place the same cameras at the exit to prove the vehicle left without being damaged. (Guests will call a day later, after they have driven 400 miles, stopped at three rest areas and a fast food restaurant to claim that the scratch on their car is from your property.)

Some hotels invest in an advanced video system that photographs all sides of the car as it is funneled into the garage or parking lot. I suggest this investment be weighed against the amount of claims you receive. It does not make sense to spend $100,000 on this system if you pay out on only five claims per year.

Reducing Obstacles

If an attendant must drive across a street, around a few light poles, into a garage and up three flights and park next to pillars, chance of damage increases with each obstacle. Whatever you can do to mark obstacles, increase lighting, and restrict other drivers and vehicles, will help.

Back It In

This is a controversial trick of the trade that most valets use. The theory is that the one who parks the car backs it in because he is not as hurried and will do it carefully. Then the retriever can drive out quicker and easier to save time.

Background Check

This is one area where drug tests are recommended. Besides that, a clean driving record is essential. Unfortunately, most of your applicants will be college-aged and have not had the driving experience or history yet, but do it anyway.

Height

This is a funny one but I learned this because I am tall. A tall valet attendant will have to adjust the seat every time, which not only irritates the guest, but increases the chance of accident because he may try to drive cramped: Knees buckled under the steering wheel. If you have a tall one, have him greet or take tickets or whatever, if you can.

The Ticket

Valets are notorious for fudging the damage diagram on the ticket. Rarely do they actually go around the car, noting damage. Or they will wait until they park it, and then it is too late. Cameras are a good backup for the damage notes.

Clearance

If your parking is in a garage, put the height clearance lines somewhere on the concourse, so the attendant will know before he even gets in the truck that that it is too tall for the garage.

Inside damage—Guests will try to claim everything from a broken window button to a transmission failure. If the vehicle is older, ask the guest if there is anything we need to know before driving it. Note any clunks, rattles, or damage inside on the ticket.

Theft Claims

It is unlikely that an attendant will steal from a car, but it is possible. The cameras mentioned above may help, but otherwise my recommendation is to do integrity checks. Those are explained in the Investigations chapter.

Do not accept vehicles for valet parking that are not securable or have exposed, unsecured items (like in the back of a truck).

Drunk Drivers

On Saturday night, when the show or party gets out, there will inevitably be someone who imbibed a bit too much and should not drive. Your company needs to have a policy to deal with this before it happens. My suggestion for a policy is that you will give the driver fair warning that he should not drive. Offer him a taxi with free storage of his car until tomorrow or to call someone for him. Even the hotel limo or shuttle can drop him off. Though you cannot hold his keys, you can certainly stall while you negotiate with him. Threaten to call the police and if that does not work, call them anyway. If he somehow gets out of your valet with his car, call the police again and provide description and license. Document this incident. If he gets in the car and crashes, all eyes will come back on the hotel that not only got him drunk but allowed him to drive.

One unfortunate incident of which I am aware involved a swanky party held at a catering venue. They hired contract security to oversee the party and the parking areas. An intoxicated woman came down the elevator to the parking area and asked directions from a security guard. He directed her to her car and even mentioned that maybe she had a little too much, but she told him she was fine. She made it about two blocks before crashing and killing herself. This was not a valet incident, but it is the same thing. You do not want your valet attendant to shoulder this burden and be responsible for someone's death. Your policy will cover you and save a life, perhaps.

Let's go over some of the components of the Valet department.

Porte-cochère

This is simply the entry point for vehicles. We generally picture an awning or overhang to protect from weather, a carpeted entrance to the lobby, maybe a doorman, and the valet station. Some smaller hotels may have this entry but it is unmanned. Either way, this is the valet world. Besides "valet," I promise: no more French.

Concourse

In a large porte-cochère, with many lanes, the concourse is the driveway, or the lanes. In large hotels, you may have seen huge concourses with four or six lanes for valet, drop-off, self-parking, etc.

The Point

This is the greeter position where the guest first drives in and either receives their claim ticket or is directed to a place for unloading.

Podium

Most smaller valet operations will have a podium that is rolled out when valet is on-duty and holds supplies such as tickets. It should not be a storage for keys—which will be explained later.

Office

The office is not really an office, but is some sort of booth like a box office where keys are stored and valet tickets are handed in by the guest for vehicle retrieval.

Keys

Doubtless, you have seen valet operations where keys are stored on a board with hooks and fastened to a podium on wheels or some other contrivance. Oddly, this condition exists at some of the swankiest venues like country clubs, fancy restaurants, and upscale Hollywood parties, for example. If you have seen these high security operations you have likely seen movies where the thief distracts the attendant—or poses as one—and easily steals a nice car. These venues obviously do not employ risk managers or security professionals. If they did, they would realize that their liability is not only for the value of the car, but to the actions of the thief with the car after it is stolen. Stolen cars are often used in other crimes such as robberies, prostitution, drug dealing—and more directly—drunk driving.

Rather than treating the keys for the value of the metal from which they are made, we need to realize that those keys contain the value of the car, its contents, the contents of the house associated with the registration and housekeys, and especially the lives put at risk in the commission of this crime and others. This only seems hyperbolic if you have not been through an investigation or a lawsuit where someone took some valet keys from your weak little metal box and stole one or more cars, then went joyriding and killed a couple pedestrians. Assume that each set of keys fits a box sitting unattended in your drive way containing a million dollars. Would you secure them any differently?

The point is that cars AND keys need to be well-secured and protected despite what insurance you have or what the disclaimer says on the back of your valet ticket.

- Or just a few minutes.
- Never leave keys in the car, in the ignition, above the visor or under the front seat.
- Avoid the use of numeric keypads to get to keys or the room with the keys.
- Use the same access control you would use on your money vault or cashier.
- Avoid the metal cabinets commonly seen in your office supply catalog. Those are for use in back-of-house areas where the risk is not as great. Mounting one of those boxes to the wall of your valet operation is like stapling money to the wall—Easy to remove and easy to pry open.

VIRUS

When I started writing this book, our biggest virus threat was Norovirus. It was not the deadliest, but the most common seen in hotels. Now that I reach this point in the book, we seem to be at the height (hopefully) of the Corona Virus D-19 pandemic. I am no more of an expert on Covid-19 than any of my readers, but our collective knowledge on sanitation measures, crowd control, and prevention have proven the flexibility of our industry and demonstrated that there is never one answer to any problem until you look at it in hindsight.

Therefore, I am going to generalize disease response in the following pages and focus on Guest safety and security for the property since most of our new normal is dictated by government. My best advice for dealing with any situation that affects the entire population is you need to follow official guidelines whether you agree with them or not. Like everything we have discussed throughout this book, imagine yourself defending your decision to ignore one of the government regulations. Anyone that died or became ill and had anything to do with you or your property would hold you accountable for breaking with current "best practices." In our current environment of political instability throughout the world, a situation like a pandemic can go beyond a health crisis. For example, there are people who believe that the government where the disease originated could have released the virus intentionally. They speculate that it could have been a test or an actual slow and systematic elimination of its enemies or competition. If you do not buy that, how about one deranged scientist who has watched too many James Bond movies and decided to see how many people he could infect and how fast it would happen. If you are still skeptical, imagine a terrorist group that is watching, learning, and seeing the effects of this pandemic and considering a similar, or even more lethal, release of a virus.

I have two pieces of good news for you before we dive in. First, you have now written your Virus response and recovery plan. Second, this plan can be adapted for use in other situations that will become clear shortly.

Virus Overview

There are several threats of the microscopic nature that can debilitate a hotel, its guests, and employees. It is possible for these diseases to be introduced intentionally as an act of terrorism, but more likely to occur naturally or spread accidentally.

In fact, our lungs are where we are most vulnerable because the smallest particles can get to us without much resistance there. Pesticides, asbestos, rat poison, and herbicides are really causing pain and suffering for many who have been exposed to them, so it makes sense that we protect our guests and employees from accidental and intentional exposure to these and other airborne poisons.

In a hardened target, we could use walls and special air handlers to keep these airborne particles out of our atmosphere, but in a soft target where everyone has access, we must rely on other protective measures. Normal security resources are not the answer, so we rely on our colleagues in the food, facilities, and housekeeping departments to help us prevent, mitigate, and recover from these situations.

Airborne

First, let's agree on a little bit of chemistry. An airborne particle such as a flu virus is not lighter than air nor is it air. But if atomized or reduced to its smallest form, it can easily travel with air. A good example of this is when someone coughs or sneezes and contaminates someone's breathing.

There are literally hundreds of substances that can be released into the air both accidentally and intentionally. The airborne threats we have seen of a criminal or intentional nature are Ricin (a by-product of Castor beans), Anthrax, Sarin, and Cyanide.

Some naturally occurring airborne poisons are viruses and bacteria like influenza and legionella.

Viruses, bacteria, and chemical compounds of all types can sicken or even kill persons. We cannot address every one of those here, but we can look at the basics of preventing accidents, the signs of airborne criminal mischief and how to react and recover from their release.

> After 9/11, several envelopes with white powder were processed through the US Postal Service. The substance was meant to resemble Anthrax, a deadly poison that, when aspirated, can kill its intended victim. Being so close in time to the terrorist

attacks, it created quite a scare. Powder-laced envelopes are still a common use for pranks, threats, and actual terroristic acts in the workplace. The motives may be political, domestic violence, or disgruntled employee related.

Fortunately, using an airborne substance to intentionally infect someone or some place is difficult and dangerous for the offender. This is evident by the number of would-be poisoners who have been found in their homes or hotel rooms dead and surrounded by some deadly legumes.

Ingested Poisons

Most of the substances mentioned above, as being dangerous when airborne, are even more dangerous when ingested as a liquid or solid. Liquid poison is known to most of us as the literary favorite for murder, but it exists in real life also.

In 2013, a physician was arrested for putting ethylene glycol in his colleague's drink to kill her. The antifreeze, which easily is passed off as a sweetener due to its color and taste is a relatively slow-acting, but effective poison that damages the kidneys.

After 9/11, when we started looking at other ways the homeland could be attacked by terrorists, the water supply was—and still is—considered one place where a poison could be introduced to harm large numbers of people.

Contact Poisons

Some poisons can do their business by permeating skin cells on contact. The most feared are mercury, toxins associated with certain animals like the puffer fish, and plutonium. Some of these have jumped off the pages of spy novels into real life, but mostly in Europe and the Middle East where some contact poisons are suspected of killing high profile adversaries.

Prevention

Three methods of exposure—airborne, ingestion and contact; several motives of release, e.g., criminal, terror, accidental and natural; and a multitude of substances—mean thousands of scenarios for which to train and prepare.

Like many threats discussed in these pages, I would expect to see poison more likely manufactured in a hotel room than being targeted at a hotel. However, many have theorized, as I opined in my opening, that terrorists would, if they could, use poison as part of an attack on a large area or multiple targets.

Like many threats being addressed here, it is more likely that the hotel would be used for its manufacture or preparation rather than being a target for its exposure. However, the intentional threat still exists, and the accidental threat is foreseeable.

Whatever the case, awareness is the best defense for a soft target. Again, a hardened target can do many things to protect its environment from these types of attacks, but not a hotel. Education for frontline employees should include some basic—and I mean basic—chemistry. Is there any normal reason for a guest to have a supply of raw beans in their room? Powdered substances in bags? Test tubes, mixing vials and the like? Any good reason to smell rotten eggs where you work? Most criminal enterprises like these are discovered by housekeepers who mentioned something to management that just did not look right.

> In 2019, a woman checked into a California hotel, mixed up some Hydrogen Sulfide, drank it, and died. When the body and scene were discovered by housekeeping, three floors of the hotel were evacuated, and a hazardous materials crew had to clean the hotel room and de-contaminate about 100 people. Hydrogen sulfide is a naturally occurring gas that is also easily manufactured. It is used in testing labs and is highly flammable. It has a colorful history as a suicide vehicle around the world.

Employees should trust their senses and react to things that are suspicious or abnormal. For example, natural gas and propane have additives so that they have a distinct smell. Hydrogen sulfide mentioned in this section smells of rotten eggs. Cyanide smells of bitter almonds. An employee knows what smells are normal in a hotel and which are not. Any smell that is not normal in your facility should be investigated.

Mitigation

Pandemics and legionnaire’s (water supply) are discussed as separate threats in this chapter. Once a dangerous chemical is discovered on your property, it becomes your responsibility to keep your guests safe. Make sure chemical release is included in your emergency plans—Chapter 4.

Norovirus

Norovirus is one of many contagious digestive tract ailments that are associated with food service and crowds. Cruise ships are susceptible because the same group of people tend to eat together, at the same places, and incubate together in enclosed spaces. Though ships get the bad rap, Norovirus is also prevalent in schools, amusement parks, and hotels. One person who carries the virus can spread it to hundreds of others, so preventing it and then mitigating it is difficult. Action must be taken, however, to keep a bad situation from getting worse. Though not particularly deadly, Norovirus, like Covid, can kill elderly, children, and those with weakened immune systems.

Your local health department will track cases of Norovirus, Influenza, and other contagious or deadly illnesses. Instances of the virus discovered in emergency rooms or doctors' offices will be reported to the Health authority and when certain triggers are met, the health department will issue alerts and voluntary or mandatory remediation protocols. This seems irrelevant after living through a pandemic, but we will have these other viral threats and even when we recover from one, we are still susceptible to others.

These triggers are subjective and decided by the doctors at the Health Department. For instance, three exposures traced to the same restaurant may trigger a property warning. Three incidents at each of three separate hotels may cause a regional alert. It is to your advantage to get in front of these alerts by getting on a first name basis with the health Department medical authorities or managers.

A city of about 300,000 hosted a national volleyball tournament for teenagers from across the nation. On the first day of the tournament, several of the kids came down with flu-like symptoms. The patients were from different hotels but had all played their games at the same venue. While the organizers blamed the outbreak on the host city and its food and employees, a quick investigation by the Health Department determined that one of the girls actually brought the virus with her on the bus and began the contamination before the tournament even started. The Health Department turned out to be an ally of the hotels and saved them some blame and reputation damage.

Preventing Norovirus

A good sanitation program in your restaurants and public areas will go a long way in preventing outbreaks of contagious diseases. These programs are labor-intensive, however, so they are often only implemented when necessary or after the outbreak is discovered.

Your head chef or Food and Beverage Director has likely been certified in proper food sanitation and knows the proper protocols very well. If not, the Health Department will be happy to share their recommendations with you. These measures are usually voluntary as long as your procedures already meet minimum health standards and unless a health emergency is established. You can bet the minimums have changed after the pandemic.

Buy-in from your public housekeeping folks is also necessary to prevent contagions from infiltrating your establishment. Preventive measures are generally a deeper cleaning and use decontaminants rather than just dusting and vacuuming. Like we instituted during Covid, one solution is to simply reduce exposure by cleaning the rooms less often.

As I mentioned before, your viral response has been written, tested, and approved already so it may just be a matter of scaling it to a regional viral outbreak like Norovirus.

Water Supply

Legionella is a form of pneumonia that preys on those with weaker immune systems like the elderly. Anyone that contracts it during their hotel stay may not develop symptoms until they return home. For this reason, it often goes undetected at the hotel. If it is traced back, it is too late to do anything for the initial victims but there will be plenty of them and the hotel is likely to shut down. This costly situation can be avoided with a water testing plan.

Legionnaire's is found in water or moist environments. It has been found in a few US hotels in the past 20 years—hotels that might have otherwise appeared "clean and green." While the bacteria can grow under almost any wet conditions, it generally likes stagnant water or un-ventilated structures. In one hotel, it was born in a cooling tower and spread through the HVAC system. In a Las Vegas hotel, it was found in the water pipes that had not been used in months (bar sinks in suites that were rarely used).

> It is a pretty rare form of pneumonia, but when it hits, it hits hard. Legionnaire's (bacteria named for the American Legion Conference in 1976 where dozens were affected) seems to surface in hotels every few years in a big way. Usually the spores grow in stagnant water or wet areas like cooling towers and the bacterium is often not discovered until it has sickened numerous people. Victims are often elderly who have weaker immune systems.
>
> Legionnaire's is expensive to prevent. But a good water treatment program will go a long way toward keeping these bacteria down. Many health departments require these treatment programs now.

One simple prevention technique is to run the water from every faucet on a regular basis so the germs cannot grow in the still pipe water. Some county and state health departments have taken this a few steps further and mandated water testing and treatment programs for large consumers of water (major hotels). These companies will generally work with a water treatment company—or the county agency directly—to test the water and treat it with germ-busting chemicals when necessary.

PROHIBITED ITEMS

There are some things that are a threat just because they are dangerous or being used in the wrong place at the wrong time. They may be used intentionally or unintentionally so I consider them a threat and recommend you keep them out.

On October 1, 2017 we learned some hard lessons. One that applies here is keeping track of dangerous items entering the hotel. With so many other lives at stake, we really can no longer afford to knowingly allow guests to bring things into the hotel that are dangerous or can cause danger if used in a certain way. Following are some items that should be prohibited in most cases.

Microwaves and Other Appliances

If you are new to the business, you might be surprised how many people bring their own cooking appliances on vacation. Rice cookers, microwave ovens, toasters, and even grills can be seen moving from parking lot to elevator. Hotel rooms are not designed for cooking or to handle high amperage appliances. The electric circuits (especially in older hotels) are designed for low amp devices like lamps and coffee makers.

Another issue with cooking in the room is the fire hazard. Carpet, bedding, lack of ventilation, lack of proper fire suppression is just not worth the risk. Cooking in the room will likely violate some fire codes, maybe even some health codes, and it stinks up the place.

Besides, some of the appliances used to cook up grandma's gumbo are the same things used to cook meth, so better for everyone to just prohibit these items from going up the elevator.

Coolers

Many hotels now prohibit coolers in the hotel rooms for two reasons. The obvious (and public) reason is that a cooler is a great way to conceal weapons and other contraband being brought into the guest rooms. The real reason is that, just like the stoves, people are looking to save a buck. Beer brought from the grocery store costs less than 20% of the price we charge at our bars. We want guests to party with us at our clubs and bars. But seriously, it is difficult to expect a bartender to serve people responsibly when they don't know how many drinks they had prior to coming to the bar.

Pizza Coupons

Not to pick on Pizza here, but restaurant delivery services tend to market to families in hotels, especially around amusement parks like Orlando, Anaheim, and tourist destinations like New York. These darn things are problematic for several reasons.

First of all, who do they think they are?! We did not build, staff, and decorate this hotel so you could prey on our guests and deter them from our restaurants.

Mainly, and more importantly, the people that distribute these coupons in your hotel are low-paid, temporary, under-the-table, non-background-checked "employees." Not the person you want roaming the halls of your establishment.

There have been many instances of persons using the coupons as their cover for door pushing or lookouts for door pushers. See Door Pushers as one of the threats in this chapter.

TRAFFICKING/PROSTITUTION

> If I know her as well as I think I do, she'll invite us right in for tea and strumpets
> – *Dumb and Dumber* Movie

It may be the world's oldest profession but our understanding of it is a little newer. Prostitution, 10, 20, maybe 30 years ago, was considered a victimless crime by most of society. Some high-profile cases in the last several years have changed that perception. We now understand the sex trade to be one of the end products of human trafficking.

While there is still some international smuggling of persons for slavery, most of it—including domestic—is sex trafficking. One series of popular movies depicted the international aspect fairly accurately, but here in the US we are far more likely to see the domestic form of trafficking that we know as prostitution.

It is hard for us to think of the typical prostitute that we see in a hotel or on the street as a victim, but we now know that most of them—almost all of them—did not come into the life willingly. Unfortunately, hotels are not only involved, but we are in it up to our mattress pads. First, let's look at a couple of typical scenarios, then we will talk about hotels.

John is staying in the hotel on business. After a long day of meetings and PowerPoint presentations, he goes to the bar for a drink. Not too many women at the bar, but just when he is about to call it a night, a young lady approaches him and asks if he wants some company. He buys her a drink and after a while they retire to his room.

John gets lucky with the woman and after some consensual sex, she suggests he get cleaned up and she will entertain him some more. While he is in the shower, she goes through his wallet, takes his cash and credit cards, puts his laptop in her big purse and scurries out of the room. Her pimp is waiting outside, and they head to another hotel to repeat the same scam.

This is called a trick roll. The victim, who may or may not be married, is unlikely to want a police investigation. He may want the hotel to investigate or even reimburse him for his loss.

At the next hotel, a similar transaction goes down. In this case, the prostitute leaves the hotel room door ajar or opens it for her pimp, who enters the room and robs the guest of his belongings. The prostitute screams and runs from the room in the off chance that she is detained, she can deny any knowledge of the crime. Again, the pimp and his lady flee the scene and the victim must decide his level of cooperation. The police—and maybe hotel management—are familiar with the suspects as they have encountered them before. But this violent felony will also probably go un-investigated when he finds out that he must write a statement and press charges.

Three college buddies are on a weekend trip celebrating the end of finals. One of the guys suggests they try a service that he used the previous summer. He assures his friends that this is a sure thing and there will be no trouble. The other men reluctantly agree, and the first man calls a number, which is routed to another state where a "dispatcher" takes his call and makes arrangements to have a girl there within the hour.

Thirty minutes later, a young lady shows up at the door. The men do not know she is 16 years old and a runaway from another state. She is now turning tricks to please her pimp who has been grooming her for this position by tossing her in the room and closing the door. On-the-job training. Or worse, he threatens to kill her mother or baby sister if she does not comply. This life is much better than the one she left back home where her stepdad molested her for the past year.

She claims to be 19 years old and of course she is from a reputable company so why not believe her? The girl dances for a while, offers the guys some cocaine she sells on the side, and strips for them. The guys are each getting their very own lap dance and are happy to pay several hundred dollars for the opportunity to each have sex with her. Two hours later, the girl leaves and goes straight to a woman waiting in an old beat-up car. This woman is a "bottom" (the pimp's trusted girl), and not only handles the new girls in the stable but acts as an insulator between the teenager and the pimp. She is chastised for only returning $400 for two hours work and immediately sets her sights on the next appointment. The teen's assigned goal for the night is $1,000. She wants to please her pimp because she knows he loves her more than the other girls in the stable.

Most prostitutes start out in dysfunctional families. It could be a difficult foster home, a home where he/she is abused, or even some mental illness on one side or the other. Then there may be drug use, truancy, criminal, or incorrigible behavioral issues. The child may be as young as ten years old, male or female, but is often a female about 15 years old. The victim arguably becomes vulnerable and takes an attitude that any life is better than their current situation. One in seven runaways is said to have been a victim of child sex trafficking.

Then along comes someone who offers them security, companionship, fun, money, even love—or all of those things. This recruitment may be through a "friend" at school or the mall or may be the pimp himself at a party. Once she makes the decision to accept his offer, she is likely taken to another city or state, so she does not change her mind. One day she is enjoying her new cell phone or bracelet and the next day she is in a strange hotel room being raped by one or more men over and over. Just like the dog who is scolded into submission, she is now an employee of the pimp and she better learn to deal with her new life.

In some cases, the person luring the child away from home is not a pimp, but a pornographer. In the case of small children, he (82% of offenders are male) may lure them personally or for teenagers he may befriend them through social media and establish a romance. Once this relationship becomes close enough, it is just a matter of time before they arrange a meet. The CyberTipLine averages over two million reports a year of child pornography. This type of exploitation is considered by its victims to be the most traumatic because images last forever.

The hotel room is the logical place for the business deal to be consummated. After all, would a pimp—or any criminal—take a victim to his house? Sure, there is the car, a park, under a bridge, but really a hotel room is just right. Hotels are classy. Nicer than home, usually, clean and convenient, and that is where the customers are.

The involvement of hotel rooms does not end there. Prostitutes have sales quotas. They need revenue streams to feed their greedy pimp or their own drug habit or just to buy things for themselves. This is where the "trick roll" comes in. What starts out as a seemingly consensual business agreement between a "trick" and his "hooker" can turn into a theft, a robbery, grand theft auto, even a homicide. In most cases, the prostitute will wait until her victim is sleeping, in the shower, or whatever and help herself to his wallet, car keys, laptop, etc. Or she may text her pimp to come to the room and help her. He is likely armed and robs the john.

Once the crime is complete, the hotel guest reports it to the hotel. "What are you going to do about it?" Of course, he does not want a police report. His wife may find out or his boss who sent him on the business trip to your hotel will embarrass him. The guest will expect some compensation from the hotel, going so far as to leave out the part where he paid for sex, and calling it a straight robbery from strangers that broke into his room.

This makes it difficult to investigate, impossible to make arrests if the suspects are found, and unlikely that business will patronize your hotel with any of its employees.

> A hotel chain was served with a $10 million dollar lawsuit by a girl who claimed she had been recruited into prostitution when she was 10 years old. Her pimp allegedly took her to the hotel where she was forced into sex up to 20 times per day. The hotel supposedly not only turned a blind eye but went so far as to have a bowl of condoms in the lobby. The girl and other victims allegedly appeared beaten and detached but were never questioned or intervened by hotel staff. This story is still early so facts are lacking but the hotel chain will have to defend itself against these horrifying allegations.
>
> At almost the same time, several other chains were also sued for similar conditions. It was asserted that the hotels should have known based on their signage, comments on social media, and reputation within the community that trafficking was taking place in their guest rooms.

As hotel purveyors, we are not idle bystanders, lamenting how horrible it is, but we are a willing accomplice in these crimes, and we have a moral and legal obligation to be more proactive. If we saw a man wrestle a purse from a woman and go to his room with it, our instincts would cause us to intervene in some way. But when we see a prostitute walk into our hotel and go to a guest room, we are more likely to smirk and elbow our co-workers in mutual understanding of the impending transaction.

Prostitution, human slavery, and trafficking, are all similar crimes because they have three particular components. Our crime triangle is turned sideways in this case. If you can eliminate any of the three persons at your hotel, you are doing a service to your community and to the exploited children.

End-User

Persons who are consumers of prostitution are called by many names. "John" and "trick" are some of the more glamorous terms, but just like drugs, demand increases supply so if we have persons seeking prostitutes, it makes the problem worse. Johns come in several forms. There are the young, dumb males that are out to party and have a good time, not knowing the crimes they are perpetuating. Then there are the predators, such as those that troll girls online, who use your hotel to meet their victims. Finally, there are the "professional" clients who know exactly what they are doing. They may ask for a certain type of female or male in a certain age range and inexperienced. These guys may be about sex but are often about violence and domination. (Imagine a 16-year-old thrown into the hotel room with one of these guys.)

Pimp

You probably have a certain image in your head when I mention pimp. You are mostly correct, but not entirely. First, as with drug sales and other street crimes, there are no prostitutes without pimps. The pimp controls territory, his victims, marketing, and security. He is like the manager of his business. Like any other business, he has some locations and salespersons that are established and do very well for him, then he has his new recruits which require more supervision but may bring in more profits. Prostitutes, who have built up tenure or a reputation with their pimp, can work alone. But if there is a young, inexperienced hooker, the pimp is likely hiding nearby. He may be obvious but will distance himself if trouble brews. He also protects his investments by making sure his ladies do not get caught or assaulted—unless that is what the client paid for.

Pimps are likely more obvious to the hotel employee than a prostitute. He probably knows your bellmen and other frontline workers and does not stray far when he sends a new girl to a room. The pimp knows that sex does not pay all his bills. He will supply drugs to the prostitute for her use or to sell to the john. He will also assist with the trick roll—described above. Some are obvious enough that they will be hanging out in your hallway or lobby, but others may just be a phone call away in their car. He will use intimidation with a john just as he does the girls in his stable. He relies on surprise, embarrassment, and humiliation to rob the john. Is a businessman going to report a trick roll to the police? No. The pimp knows that.

Victims. That's right: victims. It is hard for many of us to consider a prostitute a victim of anything, but at one point in their career they were innocent. No one knowingly chooses the lifestyle of a prostitute because it is not about sex. It is about submission, drug use, violence, and other crimes. The prostitute is at the bottom of the food chain in the enterprise of trafficking. She (or he) is the likely one to be arrested, to become addicted to heroin or crank, and be physically abused as part of her job.

Prostitutes are "recruited" in a couple different ways. Some are lured with the promise of security, rewards, and even love. They are often separated from their family and social circle by being taken to another city and forced to become reliant on the pimp for food, money, and shelter. There is no onboarding or training system. She goes to work immediately and violently, perhaps sent into a room where she is raped and beaten over and over. This will happen many times until she submits to her pimp. At some point she is in so deep that she is no longer recognizable as a "victim." This hardened criminal is the one you see walking the streets or walking onto your property to do a trick like she owns the place.

Rescuing these youngsters can only occur during that brief time between when they are kidnapped and before they are initiated as described above. There are some anti-trafficking groups that work with the police to rescue these girls and rehabilitate them, but it is difficult. There are also National groups like the National Center for Missing and Exploited Children (NCMEC). This group is devoted to finding runaways before they turn to the dark side.

Like every other business, marketing is the key to better sales. Word of mouth is the preferred method, but many still advertise the old-fashioned way. You may find business cards around your property offering massages or private dances in the room. There are also websites that still exist which advertise "call out" services.

Your bellmen, concierge, and valet employees are your most enterprising employees and rely on tips to survive. They can make a couple bucks moving luggage or they can recommend a good hooker to come to the room and earn 20 from the customer and another

20 from the hooker. This is good money and seemingly victimless. These employees need to be educated on what they are doing and then policies enforced that prohibit this activity.

Solutions

In the hotel industry, we used to look the other way, not realizing that almost all the prostitutes we saw were once kidnapped or brain washed. Now we know better. Some hotels are passive accomplices to the crimes occurring in their rooms and some go so far as to market themselves as a place where prostitution is tolerated. The legal community has also raised their awareness and lawsuits against hotels, which are becoming more common. A former prostitute or her family can sue hotels for tolerating the crimes because hotel operators know what to look for and how to prevent most criminal activities in their hotel rooms. So if your ego or your conscience will not let you take some affirmative action, then maybe your wallet will. Some of the prevention techniques I recommend are:

Hotels need to establish their own awareness campaign for employees that teaches them how to identify an at-risk youth, pimps, prostitutes, and other related criminal activity. There are indicators to look for, and while you will not catch everyone, you need to do your best to mitigate this enterprise, sending a message to offenders that this activity is not welcome here. Some of those indicators are listed herein. Also, the federal government has a program called the Blue Campaign that will help provide training, resources, and information to help at-risk youth.

Your hotel should not have policies that encourage prostitution. Charging by the hour, accepting cash, supplying condoms in the lobby (yes, this is a real thing), and other amenities meant to attract the short-term customer, are asking for trouble.

First, contact law enforcement in your community. The Federal Government has a campaign, but most states have some sort of program that involves training, awareness, and resources to help trafficking victims.

Second, ask the police how far they can go and with what information can they pursue a pimp or trafficker. Do they need physical evidence, or will they follow up on a hunch or tip? If they have a sex crimes unit, vice, or even a trafficking team, they may be more likely to accept your help. They may even be eager to work with you.

Finally, whether the police work with you or not, you can still make your employees aware of what to look for and what to do when they encounter certain triggers. Here are some examples.

Front Desk Clerks

Those that check-in guests see more than you think. A young girl, for example, who does not make eye contact, does not carry her own cell phone or money, and seems submissive to the older streetwise male could represent a problem. Your clerks can also recognize a prostitute or pimp if they see one. Make sure they are not trained to accuse guests of this behavior.

Check-in policies should be strict and closely followed. Accepting cash is fine, but only after a credit card is used to guarantee payment. Pimps do not carry credit cards or ID which enables them to stay under the radar. The credit card eliminates vagrants, prostitutes, and persons trying to avoid the law. Of course, ID should be taken as well.

Restrict walk-ins after a certain hour. Issue one key for each named guest on the folio. No more.

After check-out, flag the folio of offenders so that you can refuse service to them on their next attempted visit. Remember you have a right to refuse service to anyone as long as you are not discriminating against a protected class, but never give a reason. They know why you are refusing service; they just want an argument.

Guest-Room Attendants

The folks cleaning the room see everything. Signs of drug use, used condoms, blood, and familiar smells do not necessary equate to prostitution but when combined with other information may be enough to identify criminal activity or someone in trouble. (sex with a 15-year-old, even if no other crime exists, is illegal in most states).

If the GRA alerts you to unusual activity that is not a policy violation, just keep it in mind and check the room throughout the night for noise, smoking, and the things mentioned above. If the GRA finds drugs, drug residue or paraphernalia, blood, room damage, weapons, or other policy violations, lock the room and plan on evicting the occupants unless they can justify the issue.

After check-in there are some things you can do within your rights. If you suspect prostitution activity in a room, find another reason to evict them such as noise complaints or smoking—especially marijuana. You cannot enter a room without some exigent circumstance, but if you get a reason like noise that sounds like damage, screaming, fighting, strange odors, etc., take it. Make sure all occupants are on the registration. A visiting John will not want to give his name and definitely not his ID. Same with a visiting prostitute.

Cleaning personnel in the public areas can get in on the awareness as well. The public restrooms are a place where runaways and troubled females will hangout. They also use that place to hide from their pimp. Teach your porters to be aware of underage people in the bathroom. Some hotels and airports put signs inside the stalls offering help to runaways, slaves, and prostitutes.

Valet, Bell, and Concierge

These are the employees that are usually asked "where can I get a hooker?" They also likely know who the pimps are, where they park, and where they wait for their girls. First, they need to be trained that prostitution is not acceptable in the hotel and then what other signs to look for.

Establish and enforce policies that prevent bellmen, concierge, and valets from profiting off trafficking. Even your bartenders are likely involved, whether it is supplying free drinks to a woman who is "waiting for someone" or giving a nod of the head when a john is ready to be approached.

Your Bell person has at least one phone number of a prostitute they call when a guest asks where they can get a massage in their room. They get a commission from the prostitute and a big tip from the guest. Make it clear that this is unacceptable and terminate offenders. If nothing else, this is a conflict of interest and is just like calling their brother to give a guest a ride to the airport. It puts the hotel and the guest at great risk and should not be tolerated.

Bartenders also are privy to a lot of talk and information. Hookers may use the bar as a pick-up area and often tip well to receive references and tolerance from the bartender. Bartenders like all employees should be made aware of the consequences of looking the other way when they witness criminal activity. They can, at the very least, report prostitution to management.

Employee awareness programs without a reporting process on the back end are useless. Your eyes and ears should know what to look for, how to report it, and any other actions you want them to take.

Management has some tools it can use to counter prostitution. Follow the lead of your local police first. They may want you to back off while they work the case. If the police are waiting for the crime to occur, you owe it to your guests to take some preventive and reactive steps as follows.

Make it difficult to access the residential floors of the hotel. If the elevators have card readers, make sure they accept valid (unexpired) keys only. Restrict access to stairs and back doors (see chapter on CPTED) so that every visitor must pass through the lobby. Greet (challenge) visitors. “May I help you find something?” Let them know you are watching and will remember the face. Ideally, guests should or have to come down or call down for deliveries, visitors—and hookers. The johns and the hookers want to be invisible (unless the hotel is ignorant or complicit) so anything you can do to shine a light on this activity is better.

In 2019, a Texas woman was arrested for “compelling prostitution” (pimping) with her 15-year-old daughter and her 12-year-old friend. The woman would take the girls to a motel outside of town where they would be visited by two or three men who would have forced sex with them for money. The youngest girl alleged that this went on for eight months and that sometimes she was knocked out or passed out from the assaults.

Participate with police who are investigating trafficking. They may want to use the hotel to snare “call outs” or the bar to initiate a transaction. They can tell you what signs to look for in your community, such as certain pimps or method of attracting johns. Better to be part of the solution than the problem.

Find the online sources used by johns and hookers to arrange “dates.” Many have been shut down by the FBI, but new ones tend to pop up. Browse through those sites and search your hotel name or city or “downtown” or whatever applies, and you may be surprised to find your hotel rooms featured in the pictures there. You may also recognize some of your regular customers there. Again, looking the other way is aiding a criminal enterprise and you may be liable, not only legally, but civilly as well.

There are many other types of human trafficking and unfortunately hotels play a significant role in most of them.

Online Enticement

When an adult attempts to establish a relationship through social media with bad intentions. The victim, generally a teenager with a low self-esteem or suffering from a traumatic situation, is lured by the excitement of having a mature person that will love him/her and take them away from all the worries they have in their life. We have all seen the news reports of young victims who travel a great distance to meet their new lover and are either never seen again or are found dead. Some become victims of killers and some are turned to prostitution or some other form of slavery.

How many of these couples use our hotels to meet or even consummate their relationship? How are we supposed to tell a victim from a consenting adult? How do we help someone who does not want to be rescued from this chosen life? As I mentioned before, you will not catch everyone, but missing the obvious signs is negligent and even abetting the perpetrator.

Child Sex Trafficking

Taking minors from where they belong to a new place for the purpose of exploiting them for sex is against the law. Statistics show that most buyers of sex prefer young females and males so when the demand is high, the supply increases to meet it. The pimp, in these cases is a middleman. The “buyer” is the one who will end up harming or abusing the victim while the pimp is the facilitator or “distributor.” Child Sex Trafficking occurs in all 50 states. Traffickers generally target children with increased vulnerabilities:

> Chronic Runaways, Teens who have been sexually assaulted, abused or neglected; Drug abuse either by the child or within the household; Those with gender identification or sexual preference issues that are not accepted by the family.

Child Pornography

We all know what this is, and your hotel is being used to take the pictures, look at the pictures (and you know what that means), trade pictures—and by the way, they are using your free Wi-Fi to do it.

> Did you know your IT folks can see your Internet activity and your emails at work? Some companies put software on your company phone so they can also see your personal email and everything else you have on your phone. They also have software that can block certain websites that are not business related. This is frustrating but is for good reason. It would be bad news to find a manager was using company

resources to participate in some of these acts. It may be difficult with these blocks, to conduct investigations on visiting groups, dignitaries, prostitution, terrorism, and many other categories, but you may be able to circumvent them if you speak to your boss. Or you may want to consider another Internet connection at work. However, I would keep these blocks in place for your staff. You never know who is viewing pornography, or worse, at work. The authorities showing up there to arrest an employee or executive does not look good.

Take it a step further and see if your IT can put filters on your guest Wi-Fi. The same filters they put on employees would really hamper pimps' ability to market.

Did you know that we, as private citizens—business owners—have more power to stop prostitution than the police? As I mentioned many times in this book, the police can only enforce laws. Any time they make an intervention or take someone off the streets it is because they have met all of the elements of a crime, have a statement from a victim, a warrant, probable cause, and more. We, on the other hand, need none of that. We can refuse to rent a room based on someone's appearance, on a vague tip, or because it just does not look right. We could put a serious dent in this scourge called Human Trafficking—if we wanted to. I would challenge each of you—and your bosses—to stop playing the game and start being responsible. All there is to lose is a few room nights. Every Security professional in the hotel business that I know, would never knowingly allow this stuff to occur at their place. Well, now you know. Go make a difference.

Prostitution Glossary (Caution: Explicit Language)

Bottom girl or bottom bitch—The member of the stable with most seniority; most trusted; The bottom is most likely to be a recruiter and handler of the others in the stable
Carpet Ho—Higher class prostitute (spends her time in nice places)
Crib—Residence
Daddy—Pimp, dude
Date—a john, or time spent with a john
Ellie—L.E., Law Enforcement, 5–0
The Game—The life of someone in prostitution
Half and Half—Fellatio followed by Intercourse
Ho—Slang for whore; prostitute
Hooker—Prostitute
John—One who pays a prostitute for sex
The Life—The business of prostitution and the life that goes with it
Lot lizard—Truck stop or parking lot prostitute
Outcall—Provider comes to hotel
Pimp—One who traffics, manages, and trains prostitutes

Renegade	Prostitute without a pimp
Stable	a group of prostitutes belonging to a pimp
Street walker	Prostitute who looks for business on the street
Trick	A sex act for money; a person who pays for sex
Trick Roll	Stealing from and/or assaulting a john

DRUG USE

Drug use by itself is not much of a threat for hotels. When it is associated with other activity, it can be a big problem. Room damage, domestic fights, prostitution, and contributing to minors are all threats related to drugs. However, it is best to address those behaviors and not the drug use. Drug use by itself may be against the law but we are not victims of this crime and have no stake in enforcing it.

Guest-room attendants, who observe drugs in a room when in the normal course of cleaning it, should report it to management. It is important that GRAs never search a room for contraband. Guests have an expectation of privacy in their belongings and in the drawers and cupboards in the room. Management also has no right to search a room while someone is renting it. Using the GRA to search a room for management or security or even the police is a violation of a person's fourth amendment rights and anything found would be worthless as evidence in a crime. Make sure you have policies preventing unlawful searches and respect your guests' right to privacy.

Management should have a policy to deal with drugs seen (in plain sight) in an occupied room. One extreme would be to notify the police. Most jurisdictions will take no action unless it is a huge amount. If there is more than one person registered, they will all be able to successfully point their fingers at each other—and the police may not prosecute for possession anyway. You can find this out in advance from your police chief or city attorney.

The second option would be to evict the guest for violating hotel policy. Have them take their possessions with them.

The third option is to warn the guest that drug use and possession is not tolerated, and they must dispose of the substance if they want to stay in the hotel. Most will flush it or leave.

If minors are present or involved, that changes everything. This case should be reported to the police as there may be child endangerment charges and you do not want that on the hotel's shoulders.

Marijuana has some different nuances that are discussed separately.

Marijuana

Many states have legalized marijuana for recreational and/or medicinal use. However, no state compels a private business to allow persons to smoke marijuana on its premises. So, hotel management needs to make a policy decision to allow or forbid marijuana smoking in hotel rooms (or common areas). Here are a few facts to help with your decision:

- Marijuana smoke is an annoyance to most people and is strong enough to carry its odor throughout an entire floor.
- THC (the active ingredient in marijuana) is available, where legal, in edible and tablet form.
- Most states, that allow personal use, allow smoking in one's home only, and not in a hotel.
- Private property rights trump marijuana laws in every state—especially because marijuana is still classified as illegal by the Federal Government.
- It is difficult to explain to a guest why you allow marijuana smoke but not cigarettes, or vice versa.
- Exposing employees to marijuana smoke may be considered an unsafe practice and subject you to unfair labor practice claims.

Based on the annoyance factor alone, you might want to go with the "against" policy. Your biggest hurdle is going to be getting guests to understand the law and your policies. Most hotels handle this with the "No smoking" clause that is signed by the guest when they check in. This method is not 100% effective but will deter many, and when combined with a "deep cleaning fee," will deter some more. Include this policy in the guest-room attendant awareness program so they know to report offenders.

Parties

Many people like to rent a hotel room for the purpose of having a party. Sometimes they are planned and sometimes they are impromptu. If the room is rented for this purpose and you have forewarning, make the ground rules clear to your guest:

- Require a cleaning (and damage) deposit.
- Limit the number of guests to the safe occupancy of the room.
- Limit the prohibited items listed throughout this chapter.
- Provide a room that is away from other guests if possible. Explain noise policies and establish a curfew for music and guests.
- Make sure minors and alcohol are not combined irresponsibly.

> It was way too often that we ran across parties with minors consuming alcohol. You may find it hard to believe that in many cases, the parent rented the room for the teenager and left them unattended for their "birthday" or graduation or whatever. Invariably, we would call the police, the police would contact the parents, and guess who the parents blamed for not supervising the minors? That's right—the hotel. Though nobody buys that story, it does not hurt to have a good rapport and reputation with the police that you do not look the other way and do not condone that behavior.

Whenever you break up a party or any noise-generating guest room, be sure and wait about 15 minutes and do a follow up. Simply walk down the hall and make sure all is quiet.

Unplanned Parties

Usually by the time management finds out about a party in a room, it is already becoming a problem. Neighbors are complaining or employees have identified a complaint about to happen. You do not need to post any signs or have a separate check-in contract unless you are having a problem already. Assume that most people expect to use your rooms for sleeping and maybe a little TV or reading, but not for more than four people. In other words, no warning is required for evicting someone who violates your policies or uses the room for purposes other than attended. One warning, three strikes, refund or not, is up to you but not necessary.

Sales Groups

Your hotel likely courts businesses, athletic groups, schools, conventions, and the like to fill rooms (put heads in beds). Many of us tend to whine about certain groups that are high maintenance, which is irrational on our part because otherwise our hotel would remain empty and we might be cutting staff—or worse. Your best option is to go along to get along.

As I will say many times in this book, do not be the department of "no." You are a professional—you can work with anything. It is more likely someone is lazy than overwhelmed, in my experience. Anyway, here are some "threats" I have encountered from certain groups and demographics and how to overcome them.

With any large group, try to get a rooming list, including chaperones, leaders, or travel coordinators. This will be valuable when you encounter a problem with a guest that might be better addressed by one of his own. It also helps with getting intoxicated strays to their room.

Get in on the planning meetings for these groups. Find out what has been promised and what has been contracted and what has not. Your salespeople want to get signed contracts so they will promise some things that affect security. Maybe the Gym must be opened an hour early every day or open 24 hours for a wrestling team. Maybe a dance team has been told they can practice in the hallways and lobbies. You might expect that a large group would buy out an entire floor or be separated from regular guests, but it does not always work out that way.

Certain groups are prone to party more than others. Be prepared to deal with drugs, prostitutes, intoxicated guests, and even room damage.

Some groups come every year and always cause the same problems. From our perspective, we wonder why we keep inviting them back, but from a sales perspective, all is well. Make your concerns known and insist on some mitigation. You can require deposits for damage, reimbursement for extra security overtime, and even a "behavior contract." This works well with high school kids. Give them some ground rules like curfews, no running, boundaries, etc. Make their leadership enforce the contract and hold them accountable.

Where I used to work, we had a group that came every year consisting of high school and college males and females who went skiing during the day and came to the hotel at night. Short story: mini spring break. We had all the problems mentioned above and much worse: Room damage, drunk kids, and all the other annoyances. Each year, we increased our security and required open credit cards to pay for smashed doors, pillow fights, and overturned vending machines. We finally gave them the boot and they made their annual rounds of the other local hotels.

One year, we decided to give them another chance. They had a new security team of their own (chaperones) and were vetting their guests better—so they said. We put one of our officers with each of theirs during the peak evening times. One night at about 2 a.m., things had wound down and it was reported that the chaperones were heading to bed. A short time later, the police received a call from a 16-year-old's parent that she had intercourse in a room. Our five-minute investigation revealed a party in one room where it had occurred. The marijuana provider and fornicator in question was one of the adult chaperones! Needless to say, that group never came back, and I believe they have since disorganized.

Avoid using third party security. This can be a big problem. If they must be included, set some boundaries, reporting mechanisms, communication protocols, post orders and vetting. Check them out if you do not know them.

Speaking of checking them out, check groups with which you are not familiar. If you have a group that holds their event at various hotels, call your counterpart at the other hotel or meeting space and find out what problems and recommendations they might have.

High School groups like bands and athletic teams are a unique challenge. They often cram four to a room and run a chaperone ratio of up to 30:1. Best advice besides those things listed above is to meet with leadership and plan plan plan.

Another unique challenge is airline personnel. Your hotel competes for the lucrative contract to host pilots and flight attendants on their layovers. The airlines and the unions that negotiate these contracts are pretty demanding and most hotels will bend over backward to meet their expectations. Hotels may offer free breakfasts, exclusive lounges, Wi-Fi, and other amenities. These are not a concern for security, but some of their complaints do affect us. Pilots need their sleep and if they have noisy neighbors, you will hear about it. Same goes with smokers. I recommend segregating these folks whenever possible—if you have an agreement with them—and make sure they have a comfortable stay.

If I have not mentioned minors in the hotel enough, here goes one more time. Those persons who are under 18 have the dubious distinction of being both the instigators of some of your headaches—and the victims. You need to supervise them for both reasons.

Familiarize yourself with local laws relating to minors including—Age of being unsupervised, age they can supervise a younger child, age of consent, how criminal law treats them—i.e., for what can they be arrested? Many states give us much leeway for the sake of child safety such as holding them without a criminal charge.

It also would behoove you, especially if you deal with youths on a regular basis to connect with those agencies that deal with kids: Child Protective Services, School Police, Juvenile Courts, etc. I always found the local truant officers helpful in taking custody of minors. (They often know them by their first name.)

Of all the myriad of issues and incidents you can have involving minors, there are a couple of recommendations that are consistent for all of them.

Get them under adult supervision (not yours) as soon as possible. Start with parents, then relatives and call the police if you must, no matter what the problem is. Anything that happens to the child while he/she is under your care, is on you. Even if you do not know she is under your care, it may be on you for lack of anyone else.

Second recommendation: There is no owner's manual or hotel guideline for dealing with kids. You are not an expert or licensed or trained for that so leave it to someone else. In the absence of mom, dad, or the police, be reasonable. Feed them only if you must. Take them away from where you found them only if necessary. Touch them only if it is reasonable and necessary. Match genders or at least have a witness. Keep siblings together. Document everything, with video if possible.

Squatters

Squatters is a term I use for persons that occupy a room that has been vacated by the registered guest. This is fraud on the hotel or on the guest's credit card. …and that is what makes it difficult to prevent or catch. Here are some methods of these grifters and how to prevent or reduce your exposure.

Many of our guests check out exceedingly early in the morning. By "check out," I mean they leave without telling us. (We actually encourage this.) The door is left ajar and many times the key is even left on the dresser. Joe scammer, who is cruising your halls without your knowledge or is a pimp who just finished some business with another guest, sees the door open. He now has all day to use the room. Unfortunately, your policies allow him to call room service and charge his meal to the room. Your operator has been trained to answer the phone, "Good morning, Mr. Jones, what can I prepare for you today?" Now Joe knows the name on the room. He can call down to the front desk and extend his stay. "Just put it on the same credit card." To make matters worse, most hotels do not charge the credit card until about 3 a.m. the next day.

Variations on this crime are the method in which they get in the room or obtain the key. They may fool a housekeeper into letting them in or find the key with its folio lying around the lobby or hallway. Some guests are naïve enough to let a prostitute or other guest stay in their room after they "check-out."

The realities of this crime that makes it difficult to catch are: The fraudulent charges, if any, against the credit card make the guest the victim. When the guest calls their credit card company, the charges will be removed and then there is no victim. (Credit Card companies rarely investigate or press charges against fraudsters.) The guest is likely not to notice additional charges until they get their credit card bill in days or weeks. If it is a corporate card, it may never get discovered. If the guest has checked out properly and a squatter takes over the room, there is technically no crime. The room was paid for one night, so the hotel has no loss to report. This is a gray area that may depend on your police and city attorney. You will have to decide for each case if it's worth it.

I recommend the following to help mitigate squatting.

- Encourage guests to check out either on the TV, your app, or in person.
- If you use key drops, empty them often and check those guests out as soon as you can.
- Have your GRAs check their floors before they start cleaning: Looking for open doors, guests leaving early, DNDs, etc. This will help get rooms checked out sooner and secure the rooms from squatters.
- Require Front Desk, Room Service, and others to verify some things if the occupant orders food or requests a stayover. Obtain last four digits of credit card, verify name on card, require a "re-swipe" for stayovers.
- Get Bell, Valet, and Shuttle drivers in on the check-out. As guest is leaving, simply ask how their stay was, or if they are checking out, or whatever. Get that info to Front Desk to check them out of the room so no more charges will incur.

Sub-Letting

This is a common practice that often goes unnoticed and without incident. Guests who rent rooms, especially if they obtain a complimentary room, may allow someone to stay in the room instead. Of course, businesses do this for their traveling employees and parents do it for their adult children, but sometimes it is a homeless person, someone they do not know, a prostitute, fellow drug user, or even through an Internet deal.

Sub-letting should be against your policy because most of the persons I mentioned above will cause trouble for you. If one is not accountable with their own credit card, they are likely to damage the room, over-crowd it, and perhaps charge items as detailed above. Use the same procedures I mentioned earlier and when you find someone has been allowed to occupy a room, have them rectify it. Change the name on the room, get a new credit card, get authorization from the renter, etc. Most states have laws requiring valid registrants for hotel rooms. Use this as a tool to enforce your policy.

There are several threats of the microscopic nature that can debilitate a hotel, its guests and employees. It is possible for these diseases to be introduced intentionally as an act of terrorism, but more likely to occur naturally or spread accidentally.

In fact, our lungs must be one of our weakest links based on the class-action lawsuit commercials on television. Pesticides, asbestos, rat poison, and herbicides are really causing pain and suffering for many who have been exposed to them, so it makes sense that we protect our guests and employees from accidental and intentional exposure to these and other airborne poisons.

In a hardened target, we could use walls and special air handlers to keep these airborne particles out of our atmosphere, but in a soft target where everyone has access, we must rely on other protective measures. Normal security resources are not the answer, so we rely on our colleagues in the food, facilities, and housekeeping departments to help us prevent, mitigate, and recover from these situations.

SAFETY

I bet at least half of my readers skipped right past this section. Safety is not the most glamorous of topics and many of us consider it a necessary evil. I am here to tell you from experience to quit fighting it and go with it. If managed correctly, safety can be a heavy contributor to Security.

Safety will become a black hole of time and resources if it is not managed correctly. As I keep reminding readers in every chapter, keep your eye on the objective and your program will be effective. If you, as many seem to do, make OSHA compliance your objective, or keeping a safety coordinator busy, your program will spin out of control.

Objective

Dumb question: What is the objective of the safety program at your facility? Many of our safety professionals think it is a training outlet. Others think it is a compliance arm. I encourage you to evaluate your objective and I recommend it be something simple like "maintain a safe workplace for our guests and team members while supporting the successful operation of the business." Obviously, our main objective is always safety, but I have seen over-zealous safety and security folks almost shut down a company in their endeavor to "be compliant." Thus, I add the second part of the objective because you will not have anything to keep safe if you do not have a business. "Compliance" is also an overused term and philosophy. You would be surprised how much OSHA regulations do not apply to a hotel. They are aimed at construction sites, factories, and chemical warehouses. That is not to say hotels do not have safety rules to follow—it is just not as many—and they are all common sense anyway. In the remainder of this chapter, I will endeavor to show you what you need to be compliant, but also what you need to be effective. You can do both.

Think about your Perfect World as it pertains to safety. Employees would correct hazards as they found them, they would clean up after themselves, guests would not slip and fall, no fire alarms, and on and on. In my experience you will not be able to get to that level of safety unless you develop a "culture of safety." That means employees do not just think about safety at meetings or during inspections, but they incorporate it into everything they do. This culture will take some time and commitment and a little bit of a "stick" on management's part, but if you want to do it, it can be done.

Your alternative is to hire a safety coordinator, send him/her to OSHA classes and have monthly safety meetings. I will go over that as well.

Culture of Safety

You may have experienced the concept of town hall meetings, safety committees, inspection forms and you might agree with me that these check a box, but do not do much for general safety. Do those things if you need or want them, but I encourage you to gain buy-in with the following method.

Like everything your organization does, whether it is a new advertising campaign, a customer service initiative, or budget cuts, it starts at the top. The GM—or whatever you call him/her—must be totally "in" to safety. Most will realize the value (explained in a moment) and are happy to make this happen. They may not have a lot of time, but they will support it.

Safety Value

I mentioned in the "Perfect World" scenario that employees would be safe, basically. The value in that is there are less injuries, and less claims for damages, and the reviews and ratings go up. Note that this is where the company and the safety coordinator tend to start parting ways. The safety coordinator gets caught up in codes and classes and meetings and inspections, while the rest of us just want everyone to be safe. Bottom line here is to keep your eye on the ball—which is safety, not necessarily compliance.

Executive Team

Back to "starting at the top": Management needs to treat safety culture like it would any new program in which they invested a lot of money.

> I visited one property where the new fire inspector was doing the annual inspection of the entire property over a period of days. The safety guy would escort him around each day. Each day, when the inspector came on property, he would stop by a certain fire exit and just take a quick look. On day one he found a mop bucket stored in the stairwell, which is supposed to be kept clear. The safety guy moved it. On day two, same thing. This time the safety guy told the restaurant manager next to the stairwell to keep it clear. Day three—same thing. The fire inspector went to the director of security and said something to the effect of, "look, I have been very nice and patient but three days in a row and now I will have to start writing this up." He had a point.
>
> The security director dispatched his staff to start checking that stairwell each day to make sure it was clear. As you might agree, this is a band-aid and not a solution. The security director realized this and told the GM what was going on. How long do you think that problem existed after that? It never happened again.

For good reason, the GM has supreme authority. That is because he/she not only wants the stairwell clear to be in compliance, but he knows people could be seriously harmed if there was an evacuation and a mop bucket was in the way. She also knows that if someone does get injured in the stairwell, there would be a financial cost to the hotel. Injuries, fines from the inspector, claims for damages—over a mop bucket? Just do it right, she would say.

This is where the executive team gets their "buy-in." The GM may have to use the stick, but it will only be necessary a couple of times. That rolls downhill, right? So, a good Food and Beverage Director is going to make sure his/her hallways and stairwells are clear—not because of the safety guy or the fire inspector, but because his/her boss expects it. Soon, the Director will expect it from his/her team and so it goes. A culture starts to take shape.

The alternative to this is, the mop bucket gets moved around every day, citations may or may not be received, and no one learns the lesson of safety.

What I mean is that instead of doing safety inspections or having the safety guy review a new thing, make every employee part of safety and ownership. We talked about ownership before and this is the same. If you have engaged, caring employees, the safety will come automatically, and everyone's job and environment will be easy and comfortable.

Coordinator

You still need a coordinator or manager to head up this process, but instead of hiring an accounting person or a compliance-related employee, try hiring someone with little or no safety experience, but with incredible people skills and some training background. All the safety jargon, regulations, and programs can be learned, but the hard part is instilling it in your staff (creating a culture) and that is where the dynamic coordinator comes in. Give them some leeway and some empowerment to train employees.

Raise your hand if your company holds annual or quarterly seminars on safety, or sexual harassment, or whatever. Does anyone walk out of there thinking "I am going to do my best to make sure we have the safest hotel?" Nope. You are going to have to get creative, and once you do, it will be easy to maintain.

How about the department that does not have any safety issues on their internal inspection does not have to go to the seminar? How about departments inspect each other instead of themselves? Take your biggest safety problem (daisy-chained power strips, cracked outlet covers, or blocked sprinklers in closets) and have contests on who can find the most violations and correct them. This just brings awareness. Get the marketing or other creative department involved.

Accountability

This is the most important aspect of Safety, or any program, frankly. I went from a property that had built a culture of safety to one that just did the bare minimum of what was required and usually that was not up to standard. What I found was the second property took no ownership of safety. For example, the restaurant staff would store their extra chairs and tables in the fire stairwell behind the restaurant. Every other employee passed those chairs and tables and thought, "It is not my department." In fact, if they did say something, they were likely told "It is not your department, don't worry about it."

So, to get this going you need two things. First is support from the big boss and the executive staff. Second, you need some communication. The big boss needs to be your stick who tells the food and beverage director that storing furniture in the stairwell is unacceptable. Then you need that dynamic safety person who has to have those difficult conversations with department heads and says, "Hey this violates the fire code and we really need your help to keep the stairs clear." Easy, right? Heck no. The Food and Beverage director is going to tell you he is too busy to listen to your drivel, he doesn't have to listen to you or anyone else, and he has been storing junk there for years with no one saying anything. Sound more realistic?

This will be difficult at first, but if you have an effective leader who will support you, it will be easier. You have some responsibility also. Nobody likes the safety guy who gets in and starts making mandates that are mostly based on his opinion and does not take the business into account. Perhaps you can help the restaurant find a place to store the stairs. Or you can talk to your local fire inspector and ask what kind of leeway you have with that stairwell that was built too wide anyway. You will be surprised, that when you reach out to the inspectors, that they are much more flexible when you are proactive than when they find a violation.

For example, you may be able to paint lines on the floor that indicate storage areas for chairs—approved by the fire department. Yes, these are going to get abused as well, so you will have to enforce it. We had an events center to hold concerts and prior to each one, it had to be inspected by a fire code official. For years and years, he would come out, tell everyone the exits were blocked or inadequate, the catering staff would clean it up, and the show would go on. This worked until a new inspector came to town and started writing citations instead of having them move furniture. When he threatened to shut down a $50,000 concert, management woke up. So, we had security start making those inspections as a routine way before every concert. We took the catering manager with us and pointed out violations. Then we made that same manager accompany the fire official on his inspection. Talk about buy-in. Nothing more stressful for most people than to walk with an inspector. That problem was solved, mostly. We still had to watch it and counsel new employees that did not honor the rules.

Bottom line for accountability is get the GM on board and then talk with those department heads or room managers and see what they need to be compliant. Do not be the department of “No.” You are on their side.

Participation

After accountability comes participation. This means each department; every employee gets involved in safety. Just like you expect every employee, regardless of job description to pick up litter off the carpet and greet every guest, you also require each one to be aware of safety issues. As we discussed in Awareness, you need to make it easy and rewarding to report such things and ensure that they are addressed. What creative ways are there to do that? First, ask the employees. What hurdles have you faced when communicating with other departments? I bet you will hear things like, Facilities asked me to fill out a work order when I reported a burned-out light. Or Security asked me why I was in the elevator when it made the funny noise. Once you get past these “cultural” roadblocks, it will be natural. Facilities needs to make safety calls a priority. This may involve a conversation with them to see what hurdles they have.

Take some time to meet with each department and get them to require each supervisor and manager to walk their areas every shift looking for hazards or issues that need correction. Rather than having the safety committee do this monthly, get 100 eyes and ears on this and it will not only make your building safer, but you will establish a culture of safety.

Efficiency

Our third component to the safety plan is Efficiency. Safety is more than compliance and fire codes. That OSHA stuff protects employees after all, so what about our guests. The most common bodily injury claim we get is due to a slip and fall. These are 100% preventable. The prevention technique is to get employees aware of hazards and correct them. Employees should not only be aware of slip and trip hazards, but they must fix them. This means when you come across a puddle of water on the floor, you stop everything you are doing and make that a priority. Block off the area, get someone to clean it up. Calling on your cell phone as you walk away from it is not going to prevent a fall. I have watched hundreds of falls on video. Nothing is more embarrassing and harder to explain than to watch a guest spill their drink on the marble floor and watch several employees walk right past it without taking action. Then another guest falls. Even worse is the employee who spills the liquid and walks away.

So all employees will be required to stop their work, block the area, and clean the spill. Easy. No, not really. Employees love to justify their laziness by saying it's not my job. We have people for that, etc. What I did was, put out the policy and then the first time I saw an employee ignore a wet spill, he got written up. It did not take many of those to get the word out. I am generally pretty easy going, but those falls endanger our guests and they cost us a lot of money. There is a legal term we use called "notice." When you get a claim for a slip and fall, it is not automatic that you will be liable. If you knew or should have known the hazard existed and did not act quick enough, you had notice and did not take action. When a guest spills a drink and is followed by another who slips in it, is likely not your fault because you had no "notice" to clean it up. However, if several minutes—or hours pass by, or one or two employees walk by, then that is notice. This is why slip and falls are 100% preventable—if all employees are engaged.

Actually, employee buy-in is easy when you put these policies in context. Picking up litter is one thing, but when you explain that a spilled drink could cost the property thousands of dollars, you would be surprised at the loyalty of your folks. Notice does not just apply to puddles. Any hazard is generally judged based on whether you knew about it and did not fix it or should have known about it. Rips in the carpet, dark hallways, even strangers who do harm are considered hazards that you should be constantly looking for.

Branding

The final component is the brand of safety. This sounds corny, but what department manages safety. Is it Security? Compliance? Risk? HR? What if it was Marketing? Or Guest relations? Instead of safety being a side note to everything you do, make safety the first thing for everything you do.

Many companies actually market their commitment to safety. Then they work it into their advertising and their other commitments like service and quality. Many of us are doing this backward. We come up with a plan or a new thing and we make sure it is safe. What if we build around safety? Building a new parking garage? Want to have the one that holds the most cars or the safest one? What do guests want? I suggest asking yourself and your executives what they want. Most will see safety as a priority, especially because it pays off in the long run.

The purpose of building the culture of safety is to make the safety requirements easier and inherent rather than results of inspections or codes. We want our property to be safe for our guests and employees.

There are still some requirements and responsibilities for your safety department, so let's outline those next.

Program

In most cases, the government requires you to have a safety program in place. This does not mean that the government owns your Safety department or that the staff assigned to Safety is exclusive to those duties. I recommend managing this department as a part of Security. In my experience, having one of the administrative departments run safety takes away from its efficiency and employee buy-in. Having it at the front lines puts safety on the front lines rather than "another memo."

The program consists of four components: compliance, awareness, training, and communication.

Compliance

The safety manager is responsible for tracking regulations, codes, and recommendations and applying them to the operation of the company through the establishment of policies. The safety manager is also responsible for coordinating outside and internal inspections.

Your facilities director has just installed a new marble floor in the lobby. This floor is expensive and special and requires a certain cleaner to keep it in good shape. Naturally, he/she tells you to put out a policy that solution X will be the only solution allowed on that floor. Not so simple.

First, you are going to have to inspect the solution and make sure it conforms to the same standards that your regular stuff does. Hard to believe, but your housekeeping folks do not just go down to the store and buy a gallon of Mop 'n Glo. Their chemicals are tested for friction coefficients to prevent people from slipping and they have MSDS (Material Safety Data Sheets) sheets on that fluid so that they can get guidance if an employee gets sick or injured form using it. (More on MSDS shortly.)

Second, your written policy better not be about the value of that floor. It should be about safety. You require solution X so the floor does not deteriorate and cause accidents. (If that is true. I am not telling you to lie.)

Note: Much of this chapter involves OSHA, which is a federal agency. Your state (or tribe) may have its own safety agency that is responsible for safety in your jurisdiction. I recommend following your state's laws and standards. They will comply with Federal and probably be a little stricter in certain areas.

Outside inspections are those made by a government or regulatory agency not affiliated with the company. Inspections you may see in a hotel on a regular basis are Fire, Health, OSHA, and others depending on the jurisdiction. Private insurance companies generally inspect their client properties as well. The safety manager should accompany inspectors to take note of violations or recommendations and explain dubious practices or equipment. The safety manager will communicate these exceptions to the correcting department and document the infractions that may require a policy change or employee corrective action.

Internal inspections are those that you establish or possibly those made by a corporate entity. If you belong to a chain of hotels, corporate may have its own inspectors to see that you are complying with corporate policy and protecting the brand.

Awareness

The safety manager's job should be focused on employee involvement. It is not feasible for you to be responsible for the safety of the entire property. Instead, you should coordinate the efforts of all employees to be aware and focused on safety. There are several traditional methods of coordinating the employees and some less traditional ones.

Safety Committee

We all know that if you simply write memos and manuals and pass down information, there will be no buy-in and little or no compliance. You need to get the stakeholders—which are all of the employees—involved in the process. Safety committees are mistakenly believed by many to be an OSHA requirement. OSHA cares less how you achieve safety and more with the result. A cross section of employees is a good way to get a safety committee started.

> So, what is your biggest exposure to loss? A car stolen out of valet? Maybe a robbery of the day's receipts? Try this: In 2007, a truck driver was delivering a load of food to a retail store that had a deli. The store's grease interceptor clogged causing a slippery grease spill on the loading ramp. The truck driver slipped and suffered serious spinal injuries. She was awarded over $15 million for her fall.
>
> Every employee has a responsibility for safety. Many stores and hospitality environments maintain very strong safety programs for this reason. Spill stations, wet floor signs, immediate reporting procedures, and equipment inspection programs could have prevented this fall and this huge loss to the store and the driver.

Set a monthly meeting date with an agenda. The agenda should include a review of inspections (discussed later), new safety rules, safety suggestions, and a review of accidents or noted safety violations. Allow the committee to discuss safety suggestions that will benefit employees and reduce accidents; for example, a suggested covering for a slick walkway to avoid slip and falls.

Safety committee members will be responsible for bringing forward information from their departments, suggestions from themselves and other employees and taking this information back to their department meetings. Many consider this topic dry and send their least energetic employees. It is up to you to make the format interesting and relevant. Show the cost of accidents for the company. Pass around photos and evidence that makes the accident personal. Show the employees the effects of their recommendations and how they have prevented accidents. Prizes and awards for great suggestions or cost savings is an inexpensive motivator.

Consider bringing guest speakers like the fire marshal to speak to the committee about safety hazards and life-threatening safety problems he has seen. This goes toward that networking skill we develop and discuss further in Chapter 12.

Departmental Inspections

As I said before, the safety manager cannot do it all and would not be effective if he did. Let the employees have some empowerment over their own work area. Create an inspection form for each area so that any employee can do a regular walk-through and look for daisy-chained power strips, blocked fire exits, supplies stacked too high on shelves, etc. This provides a preinspection for officials, but more importantly, brings the awareness to the inspecting employees and all of their colleagues. These inspection forms are brought to the safety meeting and exceptions are discussed with the group to make changes.

Training

Some training is safety related for almost every department. Since this training is subject to verification by regulatory agencies, the safety manager should coordinate it. Security is one department that has a lot of safety training, like CPR. Your facilities department has even more safety training. Lockout, tag-out, welding, safety harness, and CPR are some of the classes required for your engineers. Depending on how many employees you have, this can be quite a job for you. Most managers find it easier to set up a matrix of required classes and schedule them over the year, spread out so the training is constant, but not a burden on the workforce of that department.

In early 2008, an outside contractor was hired to build a steel catwalk on the roof of the Monte Carlo Hotel in Las Vegas. During the welding, a spark landed on the exterior foam facade of the structure. The foam, which is highly flammable, was a common product used to create different textures and shapes on most hotels in that area. The resulting fire was mostly contained to the roof, but damaged the 32nd floor suites and caused evacuation of the entire building. Costs of repair and loss of revenue were reported at over $100 million.

OSHA requires that non-movable flammable structures be protected against sparks and flame during any hot work, including welding. As you might imagine, several persons and entities would be blamed for the cause of this fire.

You may be tempted to learn each of these training programs yourself and to do all of the training alone. As admirable as this is, it is not fair to the company. If something happens to you, the company will be stuck without a trainer. Spread this training over the employees who need to learn it. Have the welder teach the hot work safety class, the fountain maintenance person teach the SCUBA class, and so forth. If someone leaves, you just have to worry about that one person and that one class. Keep in mind that many agencies and even your own insurance providers provide many classes for free. Did you say "SCUBA" class? Many huge resorts and theme parks have special safety training for things like underwater breathing, rigging, enclosed spaces, and even beekeeping. Beware of your safety guy taking SCUBA classes if you have no water on your property.

Communication

Safety policies and procedures are worthless without a way to communicate them to the entire staff and sometimes guests. Remember our culture of awareness at the beginning of this chapter will make much of this unnecessary but meanwhile and otherwise you need to document the activities of your safety program. The Safety Committee is just one form of communication; here are some others.

Safety Newsletter

A safety newsletter can be a very informative way to get employees involved in safety. There is never a shortage of information that can be included in a monthly or quarterly communication. Many of the items discussed in the safety meetings can be included. Here is a list of other ideas for content:

1. Safety suggestions and rewards
2. Safety tips for employees
3. Department of the month
4. Safety tips for employees at home (weather, robbery, disaster, etc.)
5. Monthly themes for the property (October is Fire Prevention month)
6. Games that highlight safety
7. Photos of safety hazards
8. Articles from guest writers (fire chief, company doctor)
9. Safety training and class schedule

Safety Wall

At least one display or bulletin board in employee areas should be devoted to safety. Items from the safety committee and from the newsletter can be included with training class information and a place to receive suggestions.

Safety Suggestions

If given an opportunity to submit privately, many employees will be motivated to become engaged in safety in their own manner. A traditional suggestion box is just one way to encourage suggestions. Perhaps a page on the company website or a safety phone hotline will get people to become involved.

Insurance Company

Your workers' comp, business, or general liability insurance companies may be willing to provide training classes or written material, posters, and presentations on the subject of safety. Anything to make the employee more involved is of help.

Workers' Comp

We sometimes are so caught up in compliance that we forget that the objective of a safety program is to reduce accidents. I hope that you can achieve compliance while promoting safety, but the follow-up with accidents at your property is usually the forgotten step.

Workers' Compensation is simply an insurance program for employees injured at work. Sometimes it is administered by the state, but usually there is a third-party administrator or insurance company to pay medical bills and compensate for lost work time. Most hotels have a claims administrator to act as the liaison between the employees and the insurance company. This position probably falls under your Human Resources department or benefits, but there is a close relationship with the safety coordinator.

The first part of this chapter discussed prevention programs. In this next section, we will look at how accidents and claims are used as metrics for the success of the safety program.

Accidents

If not already done, there should be some level of investigation for every employee accident. This process is discussed in Chapter 8. The report should include the supervisor's statement, which answers the following questions regarding the employee's actions leading up to the accident. Has this type of accident happened before? Was the employee acting in the normal course of his or her duties? Were any policies or safety procedures violated while performing the task? Was personal protective equipment used correctly? Was other equipment used correctly? How could this accident have been prevented? Has this employee been involved in any other accident reports?

The report should also include a statement by the Engineering Department, which answers similar questions and information regarding the accident scene: hazards noted, equipment operating properly, measures that might have prevented accident, etc. Witnesses, photos, and other evidence should be included as well.

Once the report has been completed, it should be reviewed by the safety manager or coordinator. She should review all the facts to determine what action should be taken. Possible action steps include: disciplinary action against the employee for abuse of safety practices or other policies (i.e., running in the hallway); repair order for damaged or faulty equipment (i.e., loose handrail); recommendation to management for safety upgrade (i.e., replace tile floor with nonslip tiles); or recommendation for new safety procedure (i.e., carts must be pushed and not pulled).

The safety manager or, better yet, the safety team should review all accident reports (omitting personal medical information) to look for trends that might indicate a safety issue. For example, several employees have slipped in the same spot in a certain area of the kitchen. The team then comes up with recommendations where applicable, such as ergonomic training, better lighting, different flooring surface, spill stations, etc.

Other factors may lead to rises in accident reports. Some employees fake or exaggerate accidents just to get off on a busy weekend, hoping they will be paid for their time. There may be attention-getting reasons or contention with a supervisor or co-worker. The most serious reason may be insurance fraud. It is not uncommon for an employee with a chronic back or knee problem to fake an accident so he can get the needed surgery and time missed covered by the company. A good investigator should reveal these, but the safety team should be aware that no matter how good the safety program is, something like the previous examples could still lead to issues.

Your claims administrator, in an effort to reduce costs, will be very aggressive with return-to-work programs. Most employees would rather work their regular job than peel carrots or fold towels on light duty.

Documentation

OSHA requires certain reporting of accidents and other statistics related to safety. If you are tracking accidents as described previously, this should be no problem. You will not be able to accurately measure the success of your safety program unless you are tracking these incidents. Do not even think of covering up accidents or falsifying the numbers. Smaller companies do that to fly under the inspection radar, but you do not need to do that. You will not have an inordinate number of accidents if you have a program in place, and your company would not have you in your position if it wanted to keep this information from the government.

Risk Management

Somewhere along the line, safety programs were tied into risk management in hospitality venues. When you look at a brief history of guest accidents, hotels were not a very lucrative defendant for most plaintiff lawyers through the 1970s. While hotels had relatively deep pockets, accident claims were considered more of the bottom of the barrel for trial lawyers, so they were left for the struggling law firms. Insurance covered most of these cases. In the 1980s, mega resorts like the ones in Las Vegas, amusement parks, and overseas monstrosities came on the scene. With these huge facilities came more escalators, elevators, marble (slippery) floors, and the proportional increase in accidents. However, these large corporations also brought highly paid and experienced lawyers, modern video surveillance systems, and increased staff training to monitor and reduce accidents. Most importantly, the insurance deductibles for large facilities are now in the hundreds of thousands of dollars. Entire departments were devoted to the settling of accident and criminal claims.

The moral of this history lesson (subjective as it is) is that the hospitality industry is in the “deep pockets” category and we are up against experienced attorneys. We have more cases and most fall under our deductible. This makes our safety program one that is not only for guest welfare and compliance, but also for reduction and defense of risk. Some examples of safety programs or policies that reduce risk are discussed next.

Note: Of course, just about every policy mentioned in this book is designed to reduce risk. The ones here are specifically aimed at safety, but not necessarily at security. Other departments contribute to safety as well.

Restroom Logs

You have seen them in fast food restaurants, retail stores, and just about every public restroom—The Restroom Maintenance Log. These appear to be evidence that the facility is concerned with the cleanliness and stocking of paper goods. Rest assured that this is a risk reducer. A log of restroom cleaning provides several things. First, it shows the guest that someone is checking the restroom every X minutes. Second, it provides your defense that your cleaning staff cleaned up spills and other safety hazards every X minutes. Third, it provides a security defense that a set of eyes and ears entered that restroom on a regular frequency to prevent crime and violence.

You do not have to have a log on the bathroom wall, but you should have a log or schedule somewhere. If you assign a porter to clean three bathrooms all day, then you know he is in each one about a third of the time. That covers it as long as he goes back and forth to each one on his route. Be sure to assign male and female porters equally and consistently. Having a male responsible for a female restroom is not efficient, as he would have to close the restroom on each visit.

Safety Sweeps

I mentioned previously that a large retailer announces its safety sweeps on its public address system. That is a great policy (the announcements), but not necessarily for our industry. You should have a regular program of employees checking their areas for spills and safety hazards every few minutes. An employee calling in a spill to the cleaning staff is not good enough. Each employee should be trained to stand by the spill while cleaning help is called to prevent accidents.

Spill Stations

Spill stations are displays set up around your property that contain the equipment for resolving a spill or safety hazard. Generally, a broom, mop, towels, and cleaning solution with a warning cone or sign complete a spill station. The more convenient you make it for employees to take care of a hazard, the fewer accidents you will have.

Escalator Shutdown

Escalators invariably have some sort of minor issue that can lead to major injuries if not addressed. Shoelaces are caught, luggage is caught, people trip or lose their balance, and some with wheelchairs even attempt to ride them. Since escalators are not staffed by an employee, all employees need to be trained how to deal with an escalator emergency. Working the emergency stop, notifying engineers, and keeping guests off the stopped escalator are the important elements of this training. This policy will reduce accidents and keep accident severity to a minimum.

12

Technology

The Physical Protection System introduced at the beginning of this book included three components. The third was technology (or Tools or Resources). This chapter will cover many of the things that make the third leg of our security stool.

We are about to look at some of the current technologies, systems, and concepts used in Hospitality Security. Then we will explore some upcoming technologies that are likely to change our world. Hospitality and Technology are almost contradictory terms. In our industry we think of people serving people: restaurants, spas, relaxation, etc. Technology conjures images of cold, lifeless, electronic gadgets and gizmos. As I see it, the gadgets and gizmos cannot replace the human touch, but they can take on some of the support functions, administrative tasks, and repetitive procedures that free the humans to serve their guests.

It will be your job to balance technology with your human touch, using a framework of best practices to provide the safest environment possible. Some of my personal opinions on technology may help you as you develop your own opinions on this front.

I mentioned elsewhere in this book that there are different kinds of technology shoppers. Some have bigger budgets and a desire to be on the forefront of innovation, so they get every new system or product that comes along. Others wait and feel out the fabric of the industry and see what works and what does not. The final group waits until they absolutely must purchase something and are mostly limited by cost. The tools in this chapter are not grouped by cost or necessity, but rather by awareness as to what trends are out there.

GUEST SURVEYS

Granted, surveys are not the favorite part of anyone's job. I bet there is someone in your organization that lives and dies by the comments made on social media. As if that were not enough, they are probably probing guests with custom surveys to get even more feedback. I am sorry to be the one to tell you, but our industry (and other industries) has become

DOI: 10.4324/9781003037644-12

dependent on positive comments from former customers. With positive comments comes negative ones, and these are especially hard to stomach. I bet as much as you hate these surveys, when you travel you rely on Yelp, Expedia, or one of the hundreds of apps and sites that rate your prospective purchase before you buy it.

This bit about surveys resides here in the technology chapter because it has matured so drastically in the past ten years. Today, we can get instant feedback from our guests as they rate us while sitting at the table as soon as their entrée arrives. Security has a difficult dilemma with these ratings. First of all, our service is intangible, and thereby easier for someone to rate low or not at all. The restaurant might like to have feedback that said the meat was too salty or the soup too watery, or whatever, but we have no products like that, except our service.

Second, not everyone interacts with security or has a memorable meeting with an officer that compels them to write about it. Third, I think we all tend to defend our employees blindly like we would our children. "Your child was disrupting the class," "I am sure it is because your teaching methods are too boring for his advanced mind."

I think it is time we embrace this technology rather than argue with it. I have a few justifications for making this bold statement.

Guest Satisfaction

Of course, the first and foremost reason we all use surveys and comments is to make sure our guests are getting what they expect. If a guest does not feel safe or comfortable in your building, that is on you, right? There may be something you overlooked or hoped would not be that important, but get enough comments about it, and you are likely to change it or get it changed. This is not worth getting defensive because you are a company person and if it is bad for business, you do not want it.

Employee Development

Naturally, if a guest has a rude interaction with someone on your staff, you want to know about it right? If you have an employee that walks around bad-mouthing you or the brand or the food in the restaurant, you want to know it. You want to correct it. On the contrary if you get an attaboy or attagirl from a guest, that is something to celebrate. We do not always see those in our business.

By the way, this is a good time to tell you that I do not accept complaints, comments, statements, or feedback from those whom I have evicted or ejected from the property. If they did something bad enough that I do not want them around, then why would I care what more they had to say? This is not a court of law; there are no appeals or a right to "give my side." As one of my bosses used to say to these people: "If you want to talk to my boss, go to church."

Fresh Ideas

Fresh ideas on a situation are always a good thing. You may have walked by the same whatever a thousand times and a guest sees it for the first time and calls it to your attention. That again is a good thing, and something you want to fix. Besides, a guest that cares enough about a safety hazard (or whatever) is a loyal customer that will come back. Hold on to him/her tightly.

Liability

Another reason goes all the way back to Chapter 1—Risk. Remember we talked about notice. If a guest comments that the loose stones on the front walk are so loose, I almost fell, that is a gift. Fix it and thank your stars someone called it to your attention without making a claim. If you do not, that comment (which is publicly accessible), will be used against you when someone actually slips.

FIRE ALARMS

I am of the mind that Security should be responding to fire alarms, not buying them or servicing them. Chances are, you do not have any more expertise in this area than I do. This is a highly technical area that is regulated by codes and should be left to those who do that for a living. I will, however, attempt to bring you up to speed on the process of an alarm system and how to deal with it from an end-user perspective. If you are looking for the latest fire alarm technology, you will have to wait until fire codes get updated and revised every three years.

Sensors

A typical hotel has sensors to detect fire or smoke. Ion and photoelectric detectors (also known as smoke detectors), similar to the ones in your house, are used in most areas where there is normal living activity (such as hotel rooms and halls.) Other areas are covered by heat sensors, and other detectors depending on the use of the area. Unlike the sensors in your home, commercial sensors communicate to the panel and noise is generated from there. Knowing the sensor type when responding to an alarm lets everyone know what to look for when they arrive.

Panel

The sensors do not make an alert on their own. They are wired to a main Fire Alarm Panel which receives the signal, sometimes providing power to it. The panel, being a computer of sorts, provides several other functions, such as monitoring the integrity of the sensors and wiring, enunciating the location of the alarm, communicating the alarm via phone line, and various other fire management functions.

Communicator

Contrary to movies and gossip, the Fire department does not monitor alarm systems. Your alarm communicates to an alarm company that calls the fire department or whomever, depending on your instructions. The communicator in your alarm panel is a dialer that is connected to a phone line and transmits a signal based on what type of alarm it receives.

Fire alarm response is covered in Chapter 7 but you should know the basics of how the darn thing works. In addition to the components described, there may also be many more plug-ins such as exhaust fans, duct detectors and actuators, lighting, and other things about which we need not concern ourselves.

Types of Alarms

The situations that will trigger an alarm and a response from you are: Smoke Detector—expect to find actual smoke or steam, cigarettes, etc. Commercial alarms do not react to dust, bugs, and "non-fires." Heat Sensors may be found in areas that cannot have smoke detectors, like health spa and pool. They activate at about 135 degrees. Manual Pull—These are rare now in hotels because of mischief, but if you have them, realize that the only thing that activates them is a human who pulls the switch. The kitchen has a suppression system over the cooking area that is usually manually activated. The manual switch activates the alarm and empties the containers of anhydrous sulfur onto the grill. Cooks do this as a last resort because it ruins all the food and requires a thorough decontamination of food prep areas. The computer server room may have its own suppression system as well. In that case, an inert gas is discharged into the room to eliminate oxygen. There is a danger to humans in the room, but not as bad as the danger of fire. Once discharged, the danger goes down quickly.

Fire Sprinklers

I list this separate as it is one part of the alarm that is meant for suppression as well as detection. Sprinklers have a cap (in each sprinkler) that is released when the temperature in the room reaches a certain level. The temperature settings vary based on the room they are in and local fire codes. When the sprinkler activates, besides putting out the fire, water flowing through the pipes also activates the fire alarm. Though these systems are reliable—almost no false activations and quick extinguishment—the damage caused by the water is extensive.

I have never seen a sprinkler pop unintentionally. Though they are often mounted low on a soffit in a hotel (with those familiar stickers that warn of using a coat hanger on them), I have not seen one accidentally activated by a human. My experience has been when pipes freeze, break, and then thaw, causing water flow.

METAL DETECTORS

A few years ago, I would have said there is no way hotels will ever see metal detectors. That has changed recently, and we are seeing them at hotel elevators and other places.

Large resorts with large budgets and plenty of manpower have deployed metal detectors at elevators to ensure that weapons are not going up into the hotel. This is a response to the October 1, 2017 shooting where a man brought several weapons and hundreds of rounds of ammunition to his hotel room for a major shooting. There are other, more common uses for these contraptions.

Remember that metal detection is a tool used to reach an objective. You would not implement them in a soft environment unless your risks were high in that area. Some uses for these contraptions have expanded within our industry in the past decade.

Concerts

Year 2017 can be blamed for some other security-changing events as well. Two unrelated incidents of violence occurred that year that made us take another look at our processes. In May, a man detonated a bomb in the lobby of an arena in London as fans were leaving an Ariana Grande concert. The January prior to that, a man retrieved a gun he had in his luggage at the baggage claim at a Florida airport and shot 11 people. An interesting similarity between the two incidents is that both perpetrators figured out that the screening of attendees happens at the beginning and only for the "important" part. After those incidents, I saw a lot more metal detectors, and I saw them in different places.

Before Ariana, the metal detectors were placed far forward near the assembly area doors. This left out a large area of the venue that was "unprotected." There may not be as many today, but for a while it was common to see the screening point at the entrance to the assembly area. At the height of tensions in the Middle East, hotels utilized standoffs and metal detectors at the entrance to the assembly area.

Another newer area is the nightclub weapon check. After the Orlando nightclub shooting, and others, we all felt we better start inspecting everyone. Besides this, there are other places where you may use metal detectors at your place, so here are some generalities to consider for their use and placement.

It all comes back to your objective.

Deploying Metal Detectors requires a lot of manpower, training, equipment, and space. If you decide to implement metal detectors, make sure you do it correctly. Besides operation of the equipment and training those using it, you will need policies of what items are not allowed, what you do when you find them, and how to deal with them safely.

When you hear of metal detectors being used in these venues, it is generally the walk-through type. These magnet-based gantries can be adjusted for sensitivity and for approximate body location. Be careful with your guests who do not like this level of security. They will test the device, challenge its efficacy, and try to make you look ineffective.

Policy

Metal Detectors support a policy of prohibited items. The policy exists whether you have them or not, and this is just a tool to enforce your rules. You will need to post your policies on signs, your website, and perhaps on tickets, fliers, and other collateral. This may seem obvious to you, but concertgoers in Oklahoma and Arizona will bring their concealed weapons because they can. Decide how you will deal with them. New York and California will be the opposite, so know your state.

Whatever medium you use to spread this information, just be sure your clientele knows it and knows it in advance. Some suggested prohibited items are located in Chapter 5.

Placement

I cannot exactly tell you where you will place your metal detectors, but keep in mind their purpose. Concert venues, and even meeting venues, have a lobby, or a "pre-function" area. If you put the screening area in the lobby to screen only the concert area, then you will have a lobby open to threats. Your "sterile" environment will be easily tainted with bathroom breaks, food, or liquor sales, or whatever.

Put your screening as far away from your venue as possible. For example, I had a hall that was accessible only by escalators. I put the screening near the entry to the escalators. Whatever is past the screening becomes the "quarantined area" where nobody can go who has not been screened. This becomes difficult with employees, talent, and contractors. Draw your line somewhere and make sure your other access points are controlled.

Settings

Depending on what type you have, you will have to determine its sensitivity. Guns yes. What about knives? Cell Phones? Most models you purchase now will have proximity detection which tells you what part of the body the metal is located. This is useful to speed things along. Alarms on the feet can be easily ruled out without a search.

Bottles/Liquor

There are a couple reasons for prohibiting glass bottles. The obvious reason is that bottles become weapons when there's trouble. They are also a safety hazard as they fall off a riser or table and break. Liquor has been addressed elsewhere in this book, but we cannot monitor intake if someone smuggles in a bottle of their own. Finally—and maybe more importantly to your bar manager—is that we cannot sell alcohol if people bring their own.

Searches

Since the detector cannot sense bottles and it goes off each time a purse or bag goes through, we must do manual searches of bags. Generally, a cursory check of the inside of a purse is satisfactory. You are looking for guns, rockets, grenades, and bottles, not nail cutters or perfume. Have the patron open the bag and look inside. Avoid putting hands inside someone's purse. You do not know what will be attacking your fingers and she does not know if you took something. Many people use sticks or wands (like drumsticks) to put into the purse and move things out of the way. A feel of most small purses will satisfy your policy.

Decide in advance what will happen if you do find a gun. Will someone shout "gun" and everybody hit the dirt? A gun is brought through a checkpoint either by someone who forgot or someone trying to deceive you. You decide if this is an offense that means trespass, calling the police, giving the guy the boot, etc.

There are other things you will see in purses such as drugs. Forget about them. You are not the police and you are not enforcing drug laws, which are too complicated now anyway. Let it go, but practice and role play these scenarios with your staff, so they do not embarrass themselves or the patron.

> In my venue, I had to post someone at our doors who was inexperienced. He was supposed to "wand" the patrons (more on that coming up) and make sure they carried no weapons. After the wave of patrons had entered, he reported back to me with a pile of pocketknives. He said he did not know what to do, so he had confiscated them and given each guest a hand-written receipt for them. This, of course, violated our own policies and I took the blame for putting someone there with no training.

Wands

Handheld magnetometers are a common alternative to their walk-through counterparts, but not a good one. Wands are not effective because those that use them do so inconsistently and incorrectly. Even with proper training, the operators are not reliable with them. They also pose some awkward problems with cross-gender searches. If you ever watch officer's wand repeatedly, you will notice that the distance to the body is inconsistent, beeps are ignored, and bare parts are wanded the same as those covered.

In my opinion, these wands by themselves are not a reliable tool to keep guns out of your venue. They could create a false sense of security—or even negligence—if they fail to catch something.

> When my hometown concert venue started using wands, they were very diligent in setting up lines, screening, bag searches, and handheld wands. Many people did not like it because they had a no tolerance policy which meant gun toting CCW permit (permits that allow concealed weapons to be carried legally) holders and even police were turned away with their guns. This was to the least of their problems. One fellow decided to smuggle a gun in (unknown method) and then wrote to the local newspaper that the wands were just theater.

Smoking; Re-Entry; In and Out

Having re-entry at a concert or other venue requiring a screening just adds time spent for you, adds to the lines, and puts your venue at risk. Best case scenario is that someone who wants to "run to the car" is getting or taking drugs. Worst case is that they saw the holes in your security and are going back to get whatever to smuggle past your defenses. It is not necessary to offer this amenity so do not. Unfortunately, you almost have to offer a smoking area. Once through the screening, you can cordon off an area just next to the screeners or out another door, but you need to have someone to ensure that smokers are not bringing in prohibited items.

Cell Phones

Phones are a difficult item to restrict. Most entertainers do not want to see them as they are a distraction with the flash, the glow of the screen and the ringer disrupting the performance. They also can be used to record the performance and violate copyright laws if video is uploaded or shared. There is not much more to be done than to advise guests at every opportunity.

> At least one popular comedian I know, absolutely bans phones in his audiences. He fears having his act recorded and published online. He goes so far as to require they be checked in by the venue. This, as you can imagine, is beyond reasonable. There is a company that provides tamper-proof vinyl bags in which you deposit your phone at the beginning of the performance, and it is locked there until the end. A special key is provided at the exit to remove your phone. This process does not go over well, and everyone has an excuse to be exempt, including doctors, police, persons with babysitters, and so on. The comedian does not bend on this rule. If you do not like it, you can go elsewhere. We had to also patrol the event ensuring that no cell phones were out. This was easy since there were few or no phones being used.

Manpower

If you are doing the math in your head, you know metal detectors are a huge labor draw. Someone watching the detector, someone backing him up with a pat down or whatever, one or two checking bags, then you have the other doors and entrances. Employee Entrance; other doors; smoking areas; in and outdoors. Remember you have a "sterile" area and the only way to keep it secure is to watch all other doors.

CROWD MANAGEMENT

Crowd management is misunderstood by many of us and something that we are learning by trial and error. When you think about it, managing the crowd is more important than the event the crowd is gathered to see. Moving crowds of people is difficult when everything is normal, but when there is a panic, the task is dangerous and frightening. You could spend about a week at a properly formatted class on crowd management, and I recommend that you do, but in the meantime, allow me to explain a few things I have learned the hard way. In some of these cases, it is someone else who learned the hard way.

The MGM Grand in Las Vegas has an events venue to the rear of their campus that holds some of the world's boxing events, among other things. If you have not been there, a long mall-like promenade connects the lobby of the event venue to the casino. This becomes a one-way freeway of sorts with no off-ramps. At one boxing event in 2014, a temporary wall was installed to separate the crowd filing out into the lobby, from a press event also being held in the lobby. As the crowd shuffled out, the mass pushed against the temporary wall and it fell, making a loud bang which some thought was gunfire. As is often the case, the screams, and cries of "shots fired" and "gun" were louder and carried farther than the noise itself. Hundreds of people, seeking cover and trying to flee what they thought was a gunman, had nowhere to go so a classic stampede occurred.

Dozens of patrons were injured. I reviewed this case from an active shooter perspective and found that the police response was also affected by the crowd. Police responded to the main entrances of the casino and hotel and tried to get to the venue down that promenade. Of course, this was like heading east on a westbound freeway at rush hour—All in all, not the biggest crisis ever, and one that had some important lessons. We will review at the end of this section.

Crowd Management is a science that I learned by observation. Watching people's trends—where they go, how they get there, their demeanor—is fascinating to me. I find that they do not mind being "managed" if the direction provided appears progressive and fair. One big change to dealing with crowds and lines was the pandemic in 2020 when we learned how to social distance and allow space. I should say we learned it in banks and other places, but not in assembly venues because they were not opened yet.

I have narrowed my concept into three categories: Planning, Communication, and clear direction.

Planning

This seems obvious, but if you have ever been in a crowd that had no place to go, you know how frustrating it is. In traffic, we call it gridlock, and everywhere else we call it a "cluster." Your patrons rely on you being prepared and they will go elsewhere if you cannot handle it. Many people get anxious in crowds. Claustrophobia, among other conditions, causes panic which causes accidents and injuries. A bit of planning will resolve this. Planning simply requires that you have a path set for an exit from any area. It is important that the path is the same width from start to finish. If it changes, you will have a chokepoint. A chokepoint is just a funnel-like constricting of the path so that a crowd that is ten persons abreast reduces to two or three. For example, if you have a theater which has two aisles, the crowd gets up after the show and files out into the lobby. Once in the lobby, they fan out and then are funneled through the next set of doors that lead outside or wherever. That is a chokepoint that is unnecessary. If the line coming from the theater stayed the same size through the lobby to the next set of doors, there would be no need to stop, regroup, and wait for the next set of doors to handle them. There are many exceptions to this, such as wanting your patrons to buy things in that lobby, but generally, you need to plan to manage the crowd.

Communication

I do not know about you, but to me it is very frustrating to be shuffle stepping along with 100 smelly, sweaty humans, to find out there is no one managing us. Simple communication about where we are headed, why we are going there, and what will happen next alleviates anxiety and road rage. Think about those situations you have been in that are managed well. Even the TSA (Transportation Security Administration) officers, for all that is said about them, yells to you to remove laptops, fluids, and all that stuff so you understand why the line is so slow.

Direction

I cannot tell you how many times I have been in a crowd situation and been guided to nowhere or to a worsening situation. When a line comes out into an open area, what happens? People stop and look around, talk to each other, and decide where to go next. This stops or slows the line behind them. Imagine the crowd that is guided up an escalator. Everyone boards the escalator and when they reach the top, one group stops to talk about their plans. The escalator continues to unload people onto that level. Soon, patrons on the escalator are approaching the top and have nowhere to go. People topple over and it is a big mess.

In November 2008, 2,000 shoppers lined up outside a major retail store seeking to take advantage of Black Friday specials. Just before the doors were about to open, the crowd broke the doors, and trampled an employee, killing her. Arguably, this incident was not foreseeable and was considered a horrible tragedy. In fact, the major retailer avoided criminal prosecution and any civil penalties by reaching a modest settlement that included changes to procedures that would prevent the situation from occurring in the future. In the years following that event, every store in the chain implemented procedures that prevented the stampede for bargains and the chain had no further incidents. In November 2010, another large retailer had an incident very similar to the one in 2008. In this scenario, the crowd rushed the doors—also seeking bargains—and trampled a fellow shopper. Nobody was killed. What if the injured shopper was killed? Was there foreseeability? Could it be argued that the retailer was negligent? Would you like to be the lawyer or the Security Director for that store?

Besides signs and stanchions, you may need humans to direct people and stop them when necessary. Keep in mind that you have invited these people to your place, and they are your responsibility.

GUN SHOT DETECTION

You have seen these in many cities with high crime rates. The sensors placed around the city triangulate the shot and report its probable location to the police. These seem to have limited advantages because the police are too busy to respond to a crime with no suspect and no victim. This technology is now available indoors to pin down the location of an active shooter. The cost of the installation, wiring, and equipment is significant and I am not sure how effective it is or what results it could provide. One life saved would be worth the financial investment but do your own evaluation. Fortunately, it does not have a track record so you may be a ground-breaker.

ARTIFICIAL INTELLIGENCE

AI is simply the compilation of data from different sources that is analyzed by a computer to determine commonalities or relationships. In our world it might mean security databases talking to housekeeping, valet, room service, and whomever to identify suspicious behavior. Some casinos in Asia are testing this to track the movement and spending habits of high rollers. We will be there soon, but in the meantime, some of these databases might be manually compared to find anomalies.

These are just a couple of extreme examples to show, in my opinion, that tech is not always the answer. I am not saying it is bad, nor am I downplaying its efficacy. Rather I am advising to be careful of the results on which you rely and make sure the cost justifies them.

These gadgets certainly do their part to prevent future incidents—once we go on notice that an incident could occur. What we are learning now, however, is that the common denominators of all bad acts are that they are committed by humans and those humans give warnings, no matter how imperceptible they may seem. The Secret Service, FBI, foreign airports, and many destinations here in the US have already started implementing programs that focus on changing the security culture to one that is more inclusive and comprehensive.

Certainly, these and other technologies will become more advanced and play a larger role in the protection of soft targets. The trend going forward will not be to purchase more gadgets but will likely be an effort to change the "security culture." Changing the culture is no easy feat and will not happen instantly, but like 9/11, October 1 and other recent incidents are going to push us toward it.

In addition to technology initiatives such as video analytics, facial recognition, and gun-shot detection, most organizations will adopt training and awareness programs that bring all employees and guests into the security role. This is the concept I present in Chapter 11.

ANTI-TERRORISM

Hotels have been soft targets for terrorism for years—way before 9/11. Here in the United States, 9/11 brought the idea home to us that it could actually happen here. Hotels are considered "Soft" because they are not hardened to intrusion. By their nature, they are open to the public and have very little access control. They are "Targets" because they offer the opportunity to provide mass casualties, visually dramatic destruction, economic impact, and iconic news coverage.

The deaths of terror leaders in the past five years have drastically reduced the organization and success of terrorists. While attacks by foreign terrorists are down, their ability to radicalize our own citizens has risen. Unfortunately, there is still motivation to conduct simple, small-scale attacks against familiar targets that do not require extensive funding, support, and training. In recent years, we have seen numerous attempts foiled by the FBI and there is no reason to think that they (terrorists) will not continue to learn and alter their strategy based on these arrests. These and other terrorist groups are very structured in their ability to compartmentalize plans and missions while using technology like the Internet to communicate and train.

Attacks in other countries, and attempted attacks on US soil almost always include bombs (improvised explosive devices—IEDs), but some—like Mumbai—combined bombs with small arms fire. Our government authorities and oversees hotel colleagues have learned a great deal from these attacks and we have the good fortune of being able to learn and plan based on this intelligence.

In 2015, terror attacks worldwide increased dramatically. Hotels, nightclubs, and tourist venues were not exempt, because they are soft targets as described above. Attacks in the US also rose, and they were not just related to Islam.

June 2015—A white supremacist shot and killed nine people in a church in South Carolina.

December 2015—A Pakistani couple radicalized on the Internet committed an attack on a Community Center in San Bernardino, CA. Fourteen people were killed and 24 were injured.

June 2016—In Orlando, FL, a lone Islamic terrorist attacked a gay nightclub. He killed 49 people and was considered the deadliest gunman in US history (until 2017 in Las Vegas).

June 2017—A politically motivated shooter went after the Congressional Baseball Game for Charity in Virginia, US. Several people were injured, including a US Congressman.

October 2018—A White Supremacist attacked a Pittsburgh synagogue. Eleven people were killed.

March 2019—Twenty-three people were shot and killed by a Mexican-hating gunman in El Paso, TX.

These are just the deadly ones. There are plenty of other domestic groups committing lesser crimes. As purveyors of a soft target, we are on the front lines of Domestic Terrorism. Each hotel is just as likely to employ a terrorist as it is to be the victim of one, in my opinion. The hiring process and employee engagement will be as important as the physical security and awareness programs. Henceforth, I recommend following my recommendations throughout this book.

There are known cases of environmentalist, animal rights, antiabortion, and White supremacist groups that have bombed buildings, assassinated executives, and set fire to structures to raise awareness for their "cause." For our purposes, most of the measures in the last section still apply, but generally, these groups have specific targets. Intelligence and research are the keys to prevent being a target of these groups. For a hospitality venue, we need to watch what groups rent our meeting space, what executives or dignitaries visit our guest rooms, and what vendors with whom we do business.

Keep an eye on your Sales and Convention departments and make sure they inform you of every group coming on property. A simple Internet search can answer most of your questions, or at least cause you to make the appropriate alarm. You are not looking out for just the initiators of violence, but also the potential victims of it. For example, a hunting group may be targeted by an animal rights organization, or an obstetrician symposium may be attacked by an antiabortion group. Besides violence and property destruction, the last thing you want is a protest on your sidewalk by one of these groups. Specifics of Conventions are detailed in Chapter 5.

X-RAY LUGGAGE

After 9/11, many hotels started using x-ray machines for luggage that went through the main entrance. They proved expensive to maintain, were unreliable, and took too much time in the large hotels to deal with the volume of luggage. After October 1, some resorts have brought back this technology. Can you imagine the hair dryers, bottles of liquor, and all kinds of electronics that will flag on these machines and slow down the process? This is a good example of a cool technology that is used for a purpose or volume for which it was not intended. The manpower used to staff these machines would be better spent patrolling and providing high visibility, in my opinion.

BOMB DOGS

Dogs, like X-ray machines, are more of a vanity for the hotel than a practical resource. Dogs, of course, are highly effective and a great addition, but the expense is hard to justify. Also, K9 dogs require a single handler for their working life. Most security departments do not have officers with that kind of longevity. It is possible to justify the dogs but understand that bomb dogs are different from drug dogs which are different from patrol dogs you see in the back of police SUVs.

Having said that, dogs are amazing for public relations and dealing with children and most adults. Like everything else, you need to work backward from our objective. If your objective is to improve relations with guests, then a dog might be a good option. (Your local animal shelter might do you just as well for no expense.) If you are trying to prevent bomb attacks, there may be some other things to do before investing in dogs.

DATA SECURITY

This book is primarily about physical security, but we cannot ignore the convergence with data security. Those of you who deal with this collaboration might not describe it as such. These days, trying to run physical security without IT (information technology) support is like trying to be captain of a ship without an engine room. Some companies have figured this out and they put that captain in charge of his or her own engine room. Others have IT and Physical Security report to the same person. Still others are trying to work together, but with entirely different operations and agendas.

I suspect most hotels operate like the latter because they have not quite accepted that IT flows through every department and all aspects of the operation. In Security, that flow is through alarms, access control, video, reports, and admin functions, and even patrol systems. Physical Security is using more "bandwidth" and more "systems" than ever before. Convergence has been the term used in most security circles to describe the new relationship between these two entities. If you have ever had any drug recognition training, you know that convergence means two eyes working together to focus on one target. If that is true, then we do not have to look at IT as a threat or an intruder in our world, but one with whom we can collaborate to achieve a common goal. After all, one eye without the other cannot perceive depth.

Several years ago, I was embarking on a project to switch from analog to Internet Protocol (IP) cameras. My logical assumption was that I would be working with IT to transmit my data from the camera to the recording source, but also throughout the property to several end users. I called a meeting of Security, Engineering, and, of course, IT. As we gathered around waiting for the meeting to start, we all discussed with some excitement the new technology that was about to open many doors for us. The IT Director walked in quietly, went to the whiteboard, and wrote "NO" in large letters. We looked at each other and then him and asked what he meant. He said, "No, you cannot use *my* network for video." A long argument ensued about whose network it was, whose side he was on, and so on. Then he walked out.

That IT guy does not work there anymore, but that decision came too late as I had to build an entire network for video from scratch. I would have saved money, time, and probably improved the company intranet if he had been more cooperative. I hope you can learn two things from this story: One is that you need buy-in when you tromp into someone's field as I did, and two, do not act as he did when you need to work together on a project. The fact is there are hardly any projects or any equipment you will acquire where you will not need the expertise of the IT department.

You need IT probably a bit more than they need you (which may lead to some of that animosity), so build that relationship with them before you really need it. IT does not really need me to get into their office, but I rely on IT to make sure my network is up, that I have Internet and email, that my password works, and that all my systems are operating properly. I hope that you have a good person who understands we are all here to protect the assets and the guest. This is one of the first relationships you need to build if you have not done so already. My observation is that newer companies that "grew up" with IT integrate better with the department. Older companies are still utilizing IT as if it is a layer sitting on top of the infrastructure. The coalescence just has not taken yet.

Besides convergence, there is another side to data security that has nothing to do with physical security. While you may have bad guys that occasionally come into your property to do bad things, your data are under attack constantly. There are people in other countries who do nothing all day but exploit vulnerabilities in your network or data chain. If you have email, Internet, or any other link to the outside world—and you do—your data are at risk. Your data may be the most valuable asset your business has. Credit card info, personal identities, client lists, payroll, and employee lists are all on your servers and your servers all connect in some way to China, Nigeria, and who knows where else.

This is not a full-time job; worse, it is a job for an entire department of experts. For every inebriated guest or shoplifter, you physically deal with, there are another thousand attacks on your network. I am not a professional in data security, so I say leave it to the experts and support them 100%. One of the biggest risks to data security comes through employees. Either inadvertently, or intentionally, employees are responsible for most data leaks, breaches, thefts, and viruses. Your IT department should already have policies in place that address these vulnerabilities, but they are often enforced by Security—as are most thefts. Some policies regarding data security are as follows:

Confidentiality—Most employees do not leak information on purpose. It is often through a clever scam or accidentally opening a bad link. Still, everyone must sign and adhere to a confidentiality policy and be held accountable if they break it. Training sessions on scams and Internet dangers should supplement these policies whenever possible.

Unauthorized Hardware—This is often an unintentional breach as well. Employees bring in their music device or that free flash drive they received from the trade show. That device was probably made in China and its origins and intent are dubious. Companies should exclude all external drives and USB plug-ins for this reason. Besides, that sales manager who found a better job down the street just might like to supplement his income with the convention client list from your hotel. There is technology now that detects these devices being inserted into a desktop computer.

Internal Data Theft—Your employees have access to plenty and have several ways to copy data from your servers. Downloading to external drives, Bluetooth and Wi-Fi, cloud drives, and even email are some of the ways employees can pilfer client lists, personal data, and anything else the company holds dear. Even using a cell phone camera to take a screen shot is hard to detect. While your IT folks have most of these threats figured out and mitigated, they may rely on you to keep data loss from occurring.

Passwords—Password sharing is still the biggest problem for data security. Usually among co-workers, password sharing leads to some policy violations and access control issues, but when shared accidentally with outsiders, it can lead to real problems. This is one of the areas where physical security overlaps data security.

Internet/Email Filtering—Many companies have Web filters to keep workers from being distracted by nonwork-related Web sites. A more important reason is to avoid malicious sites. Just entering an unverified site can download a virus or cause other technical problems. Those filters usually are experienced based, meaning that they are not put on the exclusion list until someone finds out about it. This means an email can have a link to a malicious site that has not been vetted and can inadvertently download something bad.

One thing you do not want at work is your employees abusing the Internet. Besides being a distraction of their real work, and the possibility of downloading viruses (mentioned previously), there are some other issues. Viewing and downloading pornography, for example, could result in sexual harassment issues. What if it is child pornography or exploitation? Keeping these filters current and strict keeps everyone out of trouble.

Phishing—sending emails with malicious code or fake websites—is staying one step ahead of our cyber security brothers and sisters. I worked at one company that not only fought these attacks from every angle, but even sent their own emails to test employees. Executives on down were tempted and clicked. This is an area that you need to stay on top of and support the company.

Data Investigations

Another point of convergence for IT and Security comes in the form of investigations. Data evidence is critical in many investigations now and both departments need to work together. For example, it is common to use archived emails as evidence in a sexual harassment case. There are many systems within a hotel that house or process information that you will need from time to time. You need to set up that relationship in advance so you can get to the data quickly and cleanly when needed. A good IT department can go one step farther and alert you when problems occur. Web filters can monitor attempts to enter pornography sites, emails with key words, unusual login times and frequency, access level violations, etc. These triggers can be set in advance with a consistent response from Security and Human Resources (HR).

EMPLOYEE DURESS

Guest-room attendants (GRAs) have been complaining since the days of Mary and Joseph that there are some twisted hotel guests that exhibit bad behavior with our employees. I have been hearing these stories for 30 years, and I too, did not give them the attention they deserved. Some incidents in the news and that I am aware of personally include: Men that order towels and answer the door naked, couples who invite the GRA in to have a threesome, and invitations for drug use while working. Those may be light and funny in retrospect, but our GRAs have been hit, held captive, sexually assaulted, beaten, and even killed.

When you think about it, a lone woman employee is sent to dozens of rooms per day to meet horny business travelers, college partiers, and everything in between without even a feather duster for protection. Then there is the threat of hotel intruders who are there to burglarize rooms and run across a GRA alone and cleaning. I do not limit this threat to GRAs. Most of our hotel employees do their jobs alone whether it is Facilities, Porters, Room Service, Bell, or even Security.

After several incidents received some publicity in the first part of the 21st century, housekeepers' voices were finally heard. Thus came a few companies that improved the technology of remote panic buttons. This provides a way for employees to summon help if they are attacked in the hotel. Of course, the technology relies upon a few things. First, you need the infrastructure that provides the location of the alarm. There are systems that use existing, modern wiring, like in the entertainment system or even the thermostat, but otherwise, receivers need to be installed throughout the building.

Next, you need someone to monitor and answer the alarm. In a large hotel, that is likely security. In medium and smaller properties, it might be the operator or the front desk, who have nothing better to do than monitor one more thing. Besides that, you need to decide who responds or what happens when the alarm is activated. Do you send that front desk clerk up there? Wait a few minutes for the police?

Finally, you need a process whereby the GRA can reach her button quickly and for the right reasons.

As a different option, there are phone apps (which have some location challenges in a vertical setting), and some other technologies that share devices and infrastructures.

If you are shopping for this system, consider those factors. If you are not quite there with laying out that kind of cash, there are other things to be done to keep employees safe in the hotel.

The easiest solution is use teams, especially after hours. A pair of GRAs cleaning rooms will probably cost a little more in time because I doubt they will clean twice as fast, but it would be worth the experiment. A second option would be to schedule two on the same floor at the same time so they could at least hear each other and open rooms together, and so forth. After hours, when you have just a couple GRAs doing late check-outs and turn-downs, that could be a team. I bet your staff is already doing that because they are frightened.

Another plan that I have already noticed at many hotels is they put tons of towels, pillows, blankets, and anything else that people ask for. I am sure that cuts down on calls for service and is a convenience for the guest.

TOUR TRACKING

Tracking patrol is not a new technology, but one worth mentioning because everyone should have it. Patrol tracking goes back farther than I can say, to when guards, and even the police, carried a key and when they reached a certain station, turned the key in a clock to mark their presence. Today, we use scanners with bar codes or RFID, or if we are fortunate, we track our humans using some form of location tracker like an internal GPS.

Whatever technology you use, I recommend having it and using it all the time. First, it ensures that your employees are doing what you expect of them. Second, it documents the patrol in case we need to prove ourselves later. The contract security company may use it to show it is patrolling what they were being paid to patrol. Investigations may use it to determine the time frame for a crime. Finally, it may be used in litigation to counter an inadequate security claim.

If you have this system and it sits on a shelf or is only used occasionally, it not only becomes worthless, but could be used against you. If you have one, read the reports and make sure it is not being abused. Check the times between scans and all of the other criteria you set.

EMPLOYEE LOCKERS

Lockers are not always the responsibility of Security, but either way, you need to establish some procedures and rules.

Issuance

Lockers should be issued by someone in the company, and the name and tenant documented. The tenant will either provide their own lock of certain guidelines or use a company-owned lock. A signed form should be used that has the rules clearly laid out. No food overnight, no weapons, no company property, no animals (yes, I have seen it), no drugs or illegal items. Lockers are subject to search (check this with HR) and must be cleaned out at end of employment.

Lockers are another hassle (Like Lost and Found) that can take up a lot of time. You will need a procedure for lost keys or cutting off locks, dealing with bad smells, defacing lockers, and fighting over space. Otherwise, lockers keep personal items out of the work area which is a benefit to Security.

KEY CONTROL

Securing and issuing keys is another thankless job provided by security. If you do not yet have an automated key locker, please try to get one. The old method of using sign-out sheets was ineffective and messy and even negligent, depending on the key. Electronic cabinets are more secure, document all activity regarding the key, and can even tell you if one is missing. These cabinets can issue other property also, such as radios, ID badges, and other tools.

VIDEO

The video surveillance system formerly known as closed circuit television has come a long way since it was first used in casinos over 70 years ago. Most professionals in most security verticals agree that they need or want video systems but there is not widespread agreement on how video is best used. On top of that, lawyers, risk managers, and others have their own understanding of the uses and advantages of video—and sometimes some restrictions for you. We will unpack all of that in the upcoming sections, but first we will see if we agree on the technical aspects of the valuable tool known as video.

Known by many names, the surveillance system includes cameras, recording devices, monitors, software and associated wiring, routers, and switches. We will review each of these components, at least the ones that apply to us—the end users.

CAMERAS

Cameras are the tip of the spear for video surveillance, taking in the image, processing it to some extent, and sending it to a switch or recording device or other component for further processing. Like phones and music players and computers, cameras have evolved a great deal. Cameras have been and are still of two types.

Analog and Digital

Originally video cameras were television cameras that were re-purposed. These analog cameras instead of sending their images to a transmitter, sent them to the wire to a switch which then sent the images to a monitor and a recorder. Because they were using television cameras that used wiring instead of transmitters, they were referred to as closed circuit television. This is an oxymoron if you think about it.

Analog cameras converted the image to a radio frequency, sent that frequency through a coaxial cable, and processed it on the other end just like a television. If you are old enough to remember the old analog televisions, you recall lines of video instead of pixels. These horizontal lines were actually one continuous line, and the picture was determined by the position of the line on the screen and the brightness of that part of the line. An analog camera takes each frame of the moving image and divides it into a portion of that continuous line. This line, which consists of really just color and amplitude or brightness, is unwoven and transferred to a radio frequency. Oversimplifying this for the purpose of explanation, visualize the wave that you associate with radio frequency. The height would represent brightness and the width of the wave would be the width of the line with that amount of brightness. And this is just for Black and white. When color came about, the line was divided into squares, which were like pixels and each square had a value of blue, red, or green—still in the same line configuration. Again, this is highly simplified to illustrate the difference in the analog and digital method.

Since the analog signal is a radio wave, it is subject to interference. A stray radio signal, a bad wire, and things like that will disrupt that wave and cause the static you used to see on your big box television.

Digital cameras, instead of creating that knitted line, turn the image into pixels, which is much easier to understand. Separate your field of view into a thousand tiny dots—pixels—and assign each one a number that represents the color, brightness, and position. Send that information through the wire and then the computer re-compiles them into the same order and the picture looks the same with the same quality. Interference is seen as a loss of pixels, instead of static. As you may know, digital information, which includes video, is transmitted in a binary form, which means a series of ones and zeroes. This is important to us for a couple reasons. One is that if something interferes with the signal, a radio wave (analog) gets all beat up and causes static, but a digital signal winds up losing some pixels entirely, which is not a big deal. The computer can make up for this loss through compression or it can simply leave out those pixels.

Digital

Camera technology is changing so fast that by the time this book is published my information will probably be outdated. That is only a slight exaggeration, but I will tell you what I am seeing and what I am expecting as of this moment. Analog cameras are still surprisingly in use. That is because many companies cannot afford to upgrade and because they are exceptionally reliable and easy to deal with. Analog cameras use coaxial cable like your cable box at home. And that cable will transfer a signal indefinitely which makes it appealing. Digital cameras use networking cable or CAT5 or CAT6 which is the cable that is possibly plugged into the back of your computer at work. The downfall of this cable is that it can only transmit data a short distance before it loses definition. So, for example when we put digital cameras in our garage, we had to install switches every floor and here and there so that the signal would be transmitted back to the main switch.

Digital or Internet Protocol (IP) have some other cool advantages. They often come with an audio channel and they have firmware installed that can do the analytics that we normally use for software in our virtual matrix. A matrix is like a switchboard or a mixer, if you will, that takes all the camera inputs and allows you to put them on various monitors and play with them and things like that. A virtual matrix is the same thing, but it is software instead of physical switches. So, when the digital signals come into the server the virtual matrix allows you to move them around and do fun things with them from your PC. Analog cameras can still be used with this type of a system, but they must go through an encoder to change their signal from analog to digital.

Lens Types

My history with cameras dates to the motorized units in the casino that were about the size of a gun turret on the bottom of a B52. They were huge clunky, and you could hear them move from a few yards away. Those big, tinted bubbles were not fooling anybody. These cameras were and still are called PTZs which stands for pan tilt and zoom. And they have gotten much smaller over the years. We have all seen that the camera these days is less than the size of a pencil eraser. It is usually its housing that takes up most of the space. So, the bubbles on these moving cameras armor the size of the tip of an ice cream cone.

About ten years ago we started seeing the megapixel camera which was just a high-definition camera that worked the same as all the others. Its data took up a lot of space, but it allowed us to do things like read license plates and later, facial recognition. These multi-megapixel cameras are nothing to us anymore. But they have eliminated the need for moving lenses and Motors within the cameras. So instead of having a panning camera that covered a large room, we now put a 360-degree camera in the ceiling that has extremely high definition and it records the entire room at once, and if you want to follow someone from the front door to the back door you simply use the digital zoom on the camera and track him across the same image. This was a huge advent as it eliminated the need for those Motors which saved on maintenance, but more importantly it illuminated the blind spots. Instead of that back door being uncovered while we were looking at the front door, we can now see both at the same time. The images we get off these cameras has also improved greatly just as it has on your smartphone. We used to require infrared LEDs on cameras in dark places, but these cameras have digital irises that capture low light automatically. Of course, the 360 cameras are more expensive and are not needed in every application, such as a hallway or a small room, and so forth.

Compression

For the sake of illustration—and easy math—suppose you have a digital image in your video that is 10 MB in size. A video may use 30 of those images per second to make a good quality motion picture, which is 300 MB per second. Multiply that times 60 seconds in a minute and you have 18,000 MB or 18 gigabytes per minute. That makes an episode of your favorite sitcom 360 GB and would use a lot of storage space for 20 minutes of video.

To resolve this, our video recorders, and often our cameras, use compression. Imagine a video of a boat on the ocean. Thousands of pixels are devoted to the blue sky that hardly changes over time. So rather than repeat those thousands of pixels 30 times per second, it simply sends a command that says, "repeat the last pixel 5000 times." This saves a huge amount of space. Depending on the quality of the compression, it may read slightly different shades of blue as the same color. While this may make a difference to the beautiful cinematography in Alaska, it would not matter to an investigator researching a missing car. When you watch a streaming video on a weak connection, you may notice blocks of the image that are one color or out of sync with the movie. That is compression trying to catch up or being left behind by the movie that is using all the bandwidth.

Most surveillance systems take compression a step further and do not even bother recording images with no movement. The initial image is captured and repeated or held indefinitely until some movement changes the pixels. This phenomenon introduces us to some of the cool things that we can do with analytics. But first, more space saving.

Speed

This concept is used with analog as well as digital, but the technology is a bit different. Old analog surveillance systems recorded at about seven frames per second. To illustrate 7 fps, old television was 30 frames per second. But with video tapes, it was the only way to get video to fit on an 8-hour VHS tape. If you wanted higher resolution, you would be changing tapes every couple hour or more.

When the mega-casinos started up in Las Vegas in the early 1990s, they would deploy 1,000 or more cameras. To avoid having 1,000 video cassette recorders, they used a device called a multi-plexor that put 4, 8, even 16 channels on one cassette. Rather than have a longer tape, the multi-plexor would take an image of channel one, followed by an image of channel 2 and so on until it got to 8 or 16, then start over at channel 1. The resulting review image was a motion picture of one frame per second. If you are accustomed to watching 15 or 30 frames per second, then 1fps looks choppy. In fact, if someone was running or moving their hands quickly, you might lose the entire transaction you were hoping to capture.

As described in the inset, there were ways to save space back in the day, but you gave up way too much resolution. Many of the newer casinos hired people whose only job was to stay in the video room changing and rewinding tapes for their entire shift. Not only were big casinos elated when digital came into their lives, they were able to justify the cost of new systems with that payroll savings (of changing tapes), not to mention the ability to see stuff happening when they reviewed video.

Analytics

Video analytics is the science of using our computers to read the pixels in the images in different ways. Imagine a video monitor with thousands of pixels, as you have seen many times. The color and brightness of each pixel, along with their placement, forms an image. Now suppose you have a camera looking at a hallway and you tell the computer to alert you every time a pixel on the bottom of the screen changes before a pixel on the top of the screen. If you are expecting movement in this hallway to only go from top to bottom, you can now have the computer tell you when someone goes from bottom to top.

Next example: Suppose you want to find someone leaving a backpack unattended at an airport. You tell the computer to look for a large blob suddenly becoming a smaller blob or separating into two blobs—one that stops moving and one that keeps moving (or whatever). This could reduce the number of human eyes you need on a certain area.

Third example: Suppose you have a car that was parked in your garage for a week. It is on camera, but you are going to have to review seven days of video to find when it was burglarized. If you instruct your computer to tell you when the pixels around that car change, you can easily find when the burglary happened in a matter of seconds. Of course, there are some issues, like shadows, cars passing by, etc. But you can deal with that rather than watch hours of video.

These methods are now decades old, and the camera manufacturers have gotten creative with analytics. One retail establishment uses cameras to count barcode swipes per minute to determine cashier efficiency. They can even detect non-swipes to find collusion with shoplifters. Factories use cameras to inspect specifications and tolerances of their widgets. If the thing is supposed to come out measuring 7.723 inches, the camera can alert them if it is 7.725 inches.

Applications

Resourceful security directors have found that analytics can not only make their job easier and reduce losses, but can also save manpower, which affects the bottom line, which everyone loves. The obvious and most common use is access control. Rather than having a human watch for people jumping and piggybacking on a gate, you can have your analytics do this. There is really no limit on what can be done, it is usually a matter of somebody thinking of it and getting the manufacturer to program it for us.

In the hospitality industry, we are less concerned with access and hard targets as we are with people and their safety. So, we either use the traditional methods to save manpower to use for more complicated tasks, or, in some cases, we have taken on these complicated tasks with analytics.

Facial Recognition

You are likely familiar with this concept on some level, so let me acclimate you to where we are with Facial recognition in hotels. Let us back up to the beginning of our chapter and remember our objective. How can facial recognition help us keep guests safe? The obvious way is to keep bad guys out. If you believed television and movies, you would think that the computer could identify a face, check it against criminal databases and DMV and give you a name, a rap sheet, and warrants. This is very possible, but not likely to happen because it involves the private sector dipping into government databases. It is unlikely that you would get access to those databases. However, you could create your own, such as a database of trespassed persons. I do not know of anyone who has had efficient use of this idea.

What we are starting to see in casinos, especially in the Far East, are analytics that recognize regular players or "high rollers" and alert management to their arrival or presence in the casino. Or, if an unknown big player is seen associating with a known cheat, they can take action to prevent a crime. But the marketing folks are getting involved in the video game as well. What if your license plate reader alerted you to the arrival of a known player? The front desk begins preparing his favorite suite, the casino hosts open a parlor with a bottle of his favorite drink, etc. As he walks in the door, the camera brings up his image and you see he is traveling with his wife and kids. The pool staff is alerted and perhaps a limousine for a shopping trip is readied. A cross-check of your player database tells you that his oldest child's birthday is tomorrow, and a party is arranged.

A more practical example is the player who is identified at certain games with certain dealers. The casino can adapt their image to offer games more to his liking. These are extreme examples, but they do use facial recognition to track players.

The two problems I see with facial recognition are: (1) the challenge of a comparative database that I mentioned above, and (2) the technology is not quite perfect or at a reasonable price point. That will change very rapidly as technology always does, so be prepared, and start thinking how you would use it in your facility.

Analytics in Real Life

Let us float back down to earth after fantasizing about doing warrant checks on people coming in the front door and decide how we can employ cameras to meet our objectives. Remember that the use of any technology should either be to meet our objective (guest safety) or to free up resources so that we can use the for-guest safety.

I already mentioned access control, which is a common use of analytics on cameras. Another common one is for the investigation process or review.

Now that we understand how cameras work, let's decide how, where, and when they are deployed. It is quite common to hear someone in management say, when a crime occurs or a problem persists, to "put up cameras." Cameras are a passive tool, meaning they observe and record, but cannot do anything unless there is a human (or a robot attached). Cameras, therefore, have three uses in security.

Deterrence

The presence of a camera in some situations may act as a deterrent to would-be criminals who see it, assume someone is watching them, and decide not to do the bad thing. I give this an effectiveness score of about a 2 (on a scale of 1 to 10). First, if you have watched the behavior of criminals over many years, you know that most criminals rarely think ahead beyond the satisfaction of the crime. I have never seen a purse snatcher, for example, walk into a hotel and look up to see where cameras are pointed. They just do not plan things out. Second, if the bad guy is looking for cameras, he weighs the risk of what will happen when he does the bad thing and either puts his head down or goes to another area where there are no cameras.

Detection

A camera can detect criminal or unsafe activity all day long, but without a human (or really smart computer) watching in real time, nothing will be detected until way after the incident. In other words, you are not really protecting your guests with the presence of unmonitored cameras. In fact, you may be giving them a false sense of security by having a camera that appears to be watching them but is not. And if you are thinking about putting up those fake cameras, call your sponsor or me but stop right there. This is an awfully bad idea and can create real problems for you. What kind of area is important enough for you to put up a fake camera, but it is not important enough to put up a real one? Cameras are inexpensive now and easy to operate. Think of the woman being sexually assaulted in an elevator that has fake cameras, and her last thought being that somebody will surely be there soon because they are watching her on video. If you have any of those cameras lying around throw them away today.

Elevator Camera

Cameras in elevators have been around for years and I am still surprised to see hotels without them. Check with your elevator company because most elevators are prewired for cameras. If yours are not, consider using an analog camera that communicates on a two pair telephone wire which the elevator does have. You could also use a Wi-Fi camera perhaps or hang a long wire from the top of the elevator shaft. Just kidding on that last one. Over the last three decades I have found these cameras to be some of the most useful in the arsenal. Besides the activity in the elevator, you can also generally see the button configuration and find out what floor somebody went to or got on the elevator and get a good picture of bad guys that happened to be up in your hotel. These along with a camera at the bottom of each fire stairwell and you have got the whole tower covered.

Investigation

The third use for cameras is investigations. This is simply a review of the recorded images after an incident to determine what happened, how it happened, and who did it. It is easy to forget that we do not work for the Police Department and we are not here to solve crimes for them. Our camera system is to protect our guests and to reduce our liability. It is unlikely that you will catch any bad guys because of video. So, get that idea out of your head today. It may help with the investigation and we will certainly cooperate with the police anytime they need it. But besides the deterrent effect and the detection effect that I mentioned above we use video of an incident to determine who is at fault and what we can do to prevent it from happening the next time. For example, if you have a purse snatch in the back hallway near the stairs, the camera might reveal to you that the suspect was waiting inside of the stairwell door for the victim to walk past. This might prompt you to lock that door, increase patrols in that area, or to make some other mitigating changes. The camera is unlikely to get a good enough description of the suspect for the police to do anything, but you might find out that it was an employee, or somebody known to the hotel and get lucky in that regard. I have solved many guest injuries claims with video. Some were outright faking it, meaning it never happened. Some exaggerated the facts. I even had a video of a woman punching herself in the face in an elevator so she could claim that she was mugged. There was one famous scam were two men tried to make a false claim when one intentionally spilled water on the floor and the other man came right behind him and slipped in it. The video was priceless.

GUEST-ROOM LOCKS

In my opinion, the hotel industry is in a transition between standards for locks. For over 30 years the standard has been the magnetic stripe swipe card. There were some variations on this such as horizontal insert versus vertical insert and the size of the key, but not much else. Then a few years ago some hotels switched over to RFID keys which are the same size key with a chip embedded near the door lock, reads the key. These worked well, and I would say about half of the hotels I visit use this type of system. About six years ago some of the major hotel brands rolled out a system whereby the phone would be used to open a hotel room. This required an app on your phone in which you check in, avoiding the front desk and the hotel server pushing an encrypted code to your phone. When your phone was close to the hotel room and you activated the signal in the app, the door opened. I am not aware of any problems with this technology. It does operate on the same premise of a decentralized locks then uses near field communications that are in every smartphone, which is kind of like RFID. I went on a cruise recently that used this same technology to open the door.

Let me back up a bit and make sure we are all on the same page regarding the technology of the locks. The lock itself has a very consistent design: a mortice lock with a latch and the deadbolt that are controlled by the same handle inside. There is a servo motor inside the lock that releases a latch to allow the door to open. It does not actually slide the bolt back and forth. There are no locks that I know of that are hardwired to a central server. Instead, they operate on batteries and transmit their information through the key. The only information on the key is a numeric code that sequences for every new occupant. The key does not contain any guest information or even the room number. So how does that work? The lock is programed to accept the numeric code of the last key plus one. When the front desk goes to encode a key, the central server for room keys remembers that the last code encoded for that room was 4567 so it encodes the key with 4568. When the new guest takes that key to the room and inserts it the lock reads that the key has the next value in the sequence from the last key entered. As a safety measure once the new key is used, the last key will no longer work. There are a couple of other options that you can add to your keys such as an automatic expiration. For example, every key will expire at 2:00 p.m. on the date of check-out. This is simply encoded into the key when it is made at the front desk.

This is a fairly good system except that it is possible that the key might fit more than one room in a hotel. If 2H rooms happen to be running on the same sequence and somebody were to get lucky and try the key on that room, it would work. Odds are against it, but it could happen. The other downfall on older systems is that if you found the key there is no way to know what room it belongs to that is good for crime prevention but bad for your investigations.

You may have heard about the hotel locks that were hacked by a man at a Las Vegas hacker's convention. This certain brand of luck had a data port on its exterior which was used for programing of some sort. And where there is an opening there is a way. The hacker plugged in a device and was able to open the door electronically. You can imagine the lock company was devastated and the only fix they had immediately was to put a cover over that hole or insert a screw into it. Otherwise, I have not heard of any ways to hack these locks and I have never had anybody break into a hotel room by defeating the lock. There are some other ways that I will go over here, but I ask you to please keep them to yourself.

Since these locks are not wired to anything, they run on batteries. The batteries last a year or more, and they give plenty of warnings before they go dead. It is worth having a preventive maintenance program to change these batteries just as you do the smoke detectors in your house. If the battery dies completely, there will not be enough juice to turn the servo that opens the lock. When that happens, opening that door gets physical and the ways to open it become limited. Those methods are damaging, time-consuming, and burglars also can use them.

I was astonished to find out at one hotel when the lock had died or malfunctioned, the locksmith who is perfectly capable of getting past the lock used a car jack to spread the frame of the door. This simply pushes the door frame out away from the latch or deadbolt allowing the door to open. Maybe good in an emergency but this method damages the door frame beyond repair—because you cannot squeeze the frame back together. It is unlikely a burglar would use this method in your hotel, but why not? Another message of entering the room takes advantage of that huge gap on the bottom of the door. Several resourceful burglars have invented contraptions that we named the banjo because it had a long rigid neck with a string or wire hanging down from it. You stick this contraption like a coat hanger under the door and you get the string to go around the door handle and you pull it down. Hardly any hotel rooms have doorknobs on them anymore because of the Americans with Disabilities act, but I have seen contraptions that could turn a doorknob as well—usually with a piece of leather or rough material. I never thought much of the little safety latch on the inside of the door until I found out about this hack.

The latch tool is something every hotel security department should have. You have an emergency key for the lock and the deadbolt but if a guest is unconscious inside and the safety latches on, you need a way to get in very quickly. The safety latch tool can be homemade, or you can buy them. It is simply a flat piece of material that you insert in the open door, let it close on it, and the latch pushes out releasing the lock.

Other bad things we have seen on hotel room doors are the reverse peephole camera. This really exists and you can buy it on the Internet right now for about ten bucks. It is simply a reverse lens that goes up to the people and makes the image bigger again. This is less an invasion of the room and more of an invasion of privacy. Many of you have installed peephole blockers in response to this threat. However, on the same Internet site you can also purchase what is called an endoscope—but it is simply a camera on the end of a long rigid wire that even has a light on it. Most of them transmit their signal via Wi-Fi to your phone and these can be easily slid under the door through vents in the walls over drop ceilings and anywhere else. You have heard of people on cruise ships finding these in their cabins.

Elevator Keys

More and more hotels are installing key card readers in their elevators. This has become an industry standard as hotels are being held accountable for intruders in the residential floors of the premises. Readers would be acceptable in most cases in lieu of a live person monitoring them, but neither are fool proof nor weigh your options accordingly. There are two types of card readers in elevators. One type communicates with the key server in the hotel, and it can tell whether a key is expired (guest has checked out) and what floor the key goes to. The other model of card reader simply reads that the key belongs to that hotel. It is basically a dummy lock. Piggybacking is a problem for the second type and neither type prevents a stalker or unwanted companion from following somebody to their room. However, as with most pieces of technology, this is another layer of security that will prevent much more problems than it allows.

RADIOS

Over the years we really struggled with different types of communication devices that were not too expensive, held up to security officer abuse, and required little maintenance. When I first started out, I remember a Motorola radio costs about $800. This is a huge expense for a team of 120. When cell phones came out there was a push to talk feature that we tried—heck everybody tried it. The delay drove us crazy, and it was not as intuitive as we had hoped. So, we went back to the expensive radios for a few years. Suddenly, and I am not sure why, but radios got smaller and cheaper. We were buying good quality radios for about $150. This price was so economical that if the radio developed a problem like a bad volume control or whatever, we would just throw it away and buy another. The service caused was more than the radio itself. The other dilemma with radios is the microphone. You can go with no microphone, a solder microphone, or an earpiece which they call a surveillance Mike. The pros and cons are having no external mic or speaker means that you must have one hand on your radio all the time which can be difficult if you are in a physical situation. The shoulder Mike takes away some of that, but it puts the speaker on your shoulder where everybody can hear it. I still chuckle in my retirement as I picture those officers that walk around with their hand on their shoulder Mike as if they are ready to make a transmission at any second. Anyway, I do not recommend either of those options as you do not want your guests hearing your radio transmissions. It is embarrassing and takes away from the hospitality environment of your hotel. That leaves us with the earpiece which comes in many forms. You can have and hear peace with the microphone that pins to the chest or even goes down the sleeve. I think that is the best option and those, Fortunately, have come down in price as well. You can get those for about $20. And because of hygiene I recommend that everybody gets their own.

REPORT WRITING SOFTWARE

I think just about everybody is beyond handwritten reports and even using Microsoft Word to type their reports. The disadvantages are obvious: it takes longer, it is messier, but the worst part is that you cannot index search these types of reports. There are two or three major manufacturers of report writing software. They may also have plugins for lost and found, live dispatch, maintenance, pass down, etc. All of them are equal in my mind so if you are shopping for this improvement, go with the best deal you can get. As I said, the most important thing for me is the ability to search and pull stats. Most of them have canned reports that you can use but I prefer the ability to write my own queries. You also want to be able to search quickly in case you have an incident where you think you recognize the guest or whatever.

What I am expecting to see next is report writing software in the format of a tablet app. I tried to invent this myself, but I just do not have the skills. I am sure somebody has worked on it already and I am also confident that everyone will use this soon. The concept is like what you may have seen in doctors' offices or restaurants or even at your front desk. The guest reports an accident, the officer who goes to the scene with his tablet can take pictures, even video, take audio statements, and have the guest fill out a form directly on the tablet. The information is uploaded via Wi-Fi, and bam you have a report in real time. I am sure it is out there, I just have not seen it.

Speaking of tablets, these are already being used to get real-time images off your video system. Someone monitoring cameras can send a photo to your tablet when you are responding to a report of an intruder in the lobby, and you have immediate identification.

LICENSE PLATE RECOGNITION

License plate recognition is not a new technology, but it is getting better and cheaper and there is really no reason not to have it. LPR, as it is known, takes a picture of the license plate as it enters your property and reads the letters and numbers. The possibilities of using that data seem endless. Some examples off the top of my head: you can know how long a car has been parked, you can compare the plates against vehicles that have visited you in the past, you can mark certain license plates as trouble or wanted and have the system alert you when they come back on property. It can be used by marketing to know when a valuable customer drives in (or even the boss) and you can share the data with the police if they are looking for a stolen car or suspect.

In some cities the police have installed cameras on their vehicles that are constantly taking pictures of license plates as the police do their routine patrol. The license plate and its location are stored and when that license plate is involved in a crime or something else, the police can look in their database and see that the vehicle is usually parked at a certain address giving them a lead as to the suspect's whereabouts. This is a controversial procedure which has been challenged by civil liberties groups. Note that it is only controversial because the government is doing it. Private property is a completely different story.

ROBOTS

A few years ago, I saw some security technology companies introducing robots as a replacement or addition to live security guards. The old man in me chuckled and said that will never happen. Well, as I write this some of my colleagues have purchased robots for their hotels. Robots just like cameras in the ceiling can use video analytics to detect unwanted behavior identify troublemakers give directions and carry lifesaving equipment like defibrillators. They can detect smoke and fire, they can detect screaming and glass breaking and even gunshots. So, I have warmed up to the idea somewhat and I expect we will continue to see robots in our industry in some form or another. I do not look at them as taking away security jobs, rather I see them as a supplement to the security officer allowing him or her to do more important things. We will always need a smiling face and a warm handshake to greet our guests.

ARMED SECURITY

Security carried guns 30 or 40 years ago, and hardly anyone noticed. Today is a different story. The American Public does not even trust police with guns. A few bad apples and some dumb mistakes have left people thinking twice. If you are trying to "weaponize" your staff or you already have some guns, your Risk folks are probably crossing their fingers, at least, that nothing bad happens. Liability with armed security is a two-edged sword and can go either way. Here is an exercise you can play with yourself as easy as I can illustrate it for you. Imagine your personnel have guns. Bad guy comes in, starts shooting, but your keen-eyed officer draws his weapon, yells for everyone to get down, and shoots bad guy until he is dead. The dead guy's family is going to sue your officer, the property, the trainers, the gun manufacturer, and on and on. Same with other victims' families. But what about the teenage girl who was shot because your officer yelled out, causing bad guy to direct his aim to the officer but hits her instead. Your training, hiring, and supervision are going to be questioned and scrutinized. Seems like you cannot stay out of trouble either way. Sure, your property may win either way, but after a couple hundred thousand dollars, nobody cares about that. I am not lobbying for or against, but you can see why I cannot decide this for you. You may also see why guns are such an emotional decision with executives. Now that we have that settled, let's look at how you decide this without the emotions.

I have played this game both ways and both are difficult. In fact, managing a department with armed security officers is difficult at best. What I would like to tell you is that whether your staff carries weapons is entirely based on your risk assessment and subsequent security plan. However, it generally comes down to an executive, attorney, owner or other decision-maker who has strong feelings about guns. So the way we will approach it here is two-fold. First, I will give you some reasons or considerations to ponder as to whether guns are needed at your facility, then I will give you some of the emotional arguments and how you can meet them with fact-based information. There are no promises or magic bullets here to get you what you want, but this is my best shot (enough puns for one paragraph).

You have three choices if you want guns on your property: Off-duty police, contract security, or your own proprietary staff. I have used all three and I will address the pros, cons, and considerations to make your own decision.

We will get to the justification and necessity of having armed personnel. The three choices above are completely disparate, so it will be an easy choice for you to decide how to arm. The deciding IF you should arm is more difficult.

Off-Duty Police

Of course having the police, in uniform, at your venue is a huge deterrent. Nothing deters fights and scares away bad guys like police officers. Their training is significantly greater than anything you can provide (about four months in their academy). Their experience will generally keep them out of social trouble, like service complaints and it will also help them to recognize criminal behavior and even criminals. Cops bring their own uniforms and tools and they know how to use them. This helps your use-of-force issues. Liability arguably diminishes when the police do something. Arrests, fights, and other physical encounters will be handled better so injuries and constitutional issues will be lessened. They have broader legal powers, such as detention, protection against violence and obstruction, and reasonable searches. They can also get help quicker if stuff goes down.

> In 2008, a man went to the Pulse nightclub in Orlando, Florida for the sole purpose of killing people at the popular gay bar. As he saw the off-duty police officer at the front door, he went around him to the side door and started shooting. The officer called for help and went around to the side and engaged the suspect. Forty-nine people were killed and over 100 officers responded to what turned out to be a three-hour ordeal.

The negatives of hiring the police (over security) are cost. Plan to spend three times as much, or more for uniformed police. The city or entity that has the police has its own lawyers that protect the department, so check with them and see what the restrictions are. Some departments do not rent out officers at all. Others allow officers to moonlight, which means you will not get a uniform, but he/she will have a gun. You may have to hire a two-officer minimum. Depending on the department, they may have other rules about breaks, scope, availability, events they can work, etc. A big disadvantage for us security guys is that police officers are autonomous when they are on your property. Do not count on them to take tickets, enforce house policies, or any non-police duties. Police are trained to react to situations, rather than prevent them. And arrests may be a first resort rather than a last.

Otherwise there will be little supervision or oversight required on your part. Remember that having a police officer, for whatever post you need, is not going to be foolproof. An officer can be defeated literally and figuratively. See the text box on the Pulse nightclub shooting.

One note on liability. This is a good time to mention the liability you can have when changing security posture. Whenever you change your security posture, and by posture, I mean the amount of security you have, you will be judged at some point or another and you need to be prepared to defend it. For example, if you had X number of security officers and due to a decline in business you reduce to X-Y number of security officers, you need to have a rationalization for doing so. The same goes if you have armed security and you abruptly take away those guns, you need to have a good answer for it. Suppose the week after you take away the guns, you have an active shooter or a robbery or some other workplace violence incident involving a firearm. Somebody that got hurt is going to hold you accountable for that decision. So I am not saying not to do it but I am saying to be prepared to justify whatever it is you did. It is easy to justify increased security such as adding guns or increasing manpower or security doors or whatever. But when you reduce it, you need to be careful that it is for good reason.

Contract Security

Contract security is another direction companies turn to add forces without increasing liability. To presume there is no liability because they are not your employees is not always true. Many times, the liability falls on the entity that hired security and not the security company. Some contract security companies offer armed security officers. You need to take a close look at several components of their program before just calling one. I have seen many companies where the officers were as I mentioned before: bring your own gun and do you have experience? This is not what you want as your foundation for use of force: asking for two guys with guns. Even the reputable companies do not necessarily have extensive firearms training programs. You may think this is not your problem, but I assure you it is. For one thing, your reputation and the reputation of your company is riding on the line when you bring a $15 an hour employee into your establishment carrying a loaded firearm. You don’t know this person, you have not worked with this person, and you do not know his training. Something bad happens even if it was with good intentions, and judgment comes down on you and your company. When I have hired a contract security company and wanted to have them armed, it was always with a company where I knew the training was above and beyond what the state requires and was sufficient enough to satisfy me that these officers knew how and when to handle their firearms. If you are going to hire armed security in this manner, take some time to find out their training, what background checks they do for their employees, and if they use their own equipment or use company equipment. In other words look at my recommendations throughout this chapter for ways to vet these armed officers.

You may be asking yourself, “Why on earth would I order up a couple of armed officers for my little hotel?” For that I give you the example of the 2020 summer riots. As you may know two retired police officers were shot in separate incidents trying to protect the family business. One was hired to stay and watch and the other was doing it as a family.

Proprietary Security

Remember the risk assessment we did in the first chapter of this book? I know you do not so I will briefly simplify it for the gun argument. The risk assessment takes two variables into account—probability and severity. A person waving a gun around on your property ranks pretty high on severity, so we are halfway there. Likelihood is a little more subjective and depends on many factors which are different for everyone. Here are some factors that make likelihood rank higher.

You may have already asked yourself, "What is my exposure if I arm my security officers?"—accidental shootings, excessive force, etc. But have you asked yourself, "What happens if I do NOT arm my officers?" That list of answers might be longer. If you have had some violent crimes in your parking lot, for example, will a victim come along and sue you for inadequate security because you did not have guns to deter these crimes or respond to them? Here is a short list of things to consider:

- A history of shootings, gun calls, or other violence on your property.
- Domestic violence calls at your property.
- Your location or environment. Urban with criminal behavior nearby, convenience stores, apartments, depressed neighborhoods, etc.
- Police response. More on this later but consider response time and type of response.
- Presence of VIPs, politicians, celebrities, etc.
- Security Posture—The visible message you are trying to convey: Guest comfort.
- Insurance provider—They may prefer weapons or absolutely prohibit them.
- Contract Security vs. Proprietary.
- Current political and economic climate.

A history of violence of any sort within your property, or even just outside, is a factor that contributes to the case for guns. Your decision makers need to decide if they are comfortable knowing of those predictors and not taking any action to ensure the safety of guests who may get caught up in a situation involving guns. I worked at a hotel that was in an urban environment surrounded by weekly motels, some retail and convenience stores. Though violent crime was not that heavy at the hotel, it was all around. Sometimes it would spill over. Sometimes robbers would run through our property to elude the police, and on several occasions the police would chase suspects and tackle them in our lobby (not the visual you want your guests to have on their vacation). This type of event does not necessarily show on your research of crimes in the area or calls for service. Though we had a really skilled police department, the side effect of them catching so many criminals was the disruption of our leisure activities. So, what does this have to do with armed security? In this example, the security was armed. Though we did not allow any cowboy involvement with the police, and they did not expect it, our employees and guests felt more at ease knowing there were armed good guys to deal with then bad guys carrying guns onto our property.

Arming security officers is often an ego device for someone like an owner or executive. Or perhaps the security chief is a retired police officer, FBI or other law enforcement. Arming security because one commanded police officers does not compare. Police officers are generally career employees and have years to train and gain experience. They are less likely to risk their job misusing a gun. Police have way more time and money to train. Even if we could train security officers for three or four months, with our comparably low pay and turnover, it would be a waste of time. If you had a security officer with the skillset and intellect to carry a gun effectively, he/she could just go to the local police department for their career.

Police officers also follow different laws and policies than we in the private sector. A police officer who makes a mistake has immunity in some cases. And in other cases, look at what happens when the police do misuse their weapons or use excessive force. Riots, calls for defunding, and other drastic solutions come from the anti-police. This type of attention would put a private business out of business.

Having said that, a private business can run an armed force effectively and safely if they followed my (or an equally good) program. I ran a program for about 12 years without a shooting and without a lawsuit regarding the use of firearms. It can be done, but not easily. It takes a commitment to safety.

Before considering arming your security staff, have a frank discussion with your executive team or counsel and include the following questions or topics.

Do we need guns? Has there been a shooting here or nearby? Any likelihood of persons using guns on our property? Your counsel may agree that another shooting is foreseeable and recommend armed security to mitigate the threat.

Will your guests accept visible guns? Should we go with a police-style uniform with holster or a coat with a concealed handgun? Some guests find it comforting to have highly trained, armed officers protecting them. Others get a little leery when they see non-police with guns. They think, this place must be really dangerous. And a few do not like the police at all under any circumstances so uniforms with guns would not be accepted.

How is your employee pool? If you arm everyone, you will lose some employees to background, some to skill level, psychological, and personal preference. Can you afford to lose them? Will they buy in to the program?

Ask your counsel if you have some liability for putting an unarmed officer in harm's way, such as a parking garage that has a history of crime. Will you be accountable to him/her or their family if something happens to him/her if they do not carry some protection.

Do we need to arm everyone? Many properties just arm certain posts, such as those working outside, or management, or specially trained officers.

Is the company willing to support the training commitment, which is extensive? Arming security with guns is not like selecting décor for a guest room. You cannot compromise on quality. Training, equipment, and personnel have to be top-notch. This would be my recommendation.

Ask your insurance company what they think. Guns may be a welcome risk mitigation, or they may consider them an unnecessary risk. They will be concerned about accidental shootings, excessive force, and other problems. We can comfort them on some of these items but most have an opinion that goes one way or the other and never come to the middle.

Ask your executive team about publicity. It may be good in your region to have armed security, or it may be frowned upon. How will you deal with a shooting—good or bad—that brings negative publicity.

I will address some of these issues as we move forward, but some of them will require decisions made at your property.

I was fortunate enough to manage an armed security program that had NO problems. We had no accidental shootings—in fact, we had no shootings at all. We pointed them at a few people—sometimes for good reason and sometimes not—but each situation ended peacefully. Some might say we did not need guns if we never shot them at anyone. I believe the opposite is true. People noticed our guns, and some commented on it. Some raised eyebrows, some thanked us for keeping them safe. Some thought we were police. Like most deterrence measures in security, it is hard to measure efficacy. It is safe to say, the positives far out-weighed the negatives.

This good experience with an armed staff was not accidental. It takes constant effort with training, discipline, hiring, equipment, and management. I was fortunate to have a great team that made me look good in many ways. So let me show you how we did it effectively.

Hiring

You may look at your current staff and think, no way are these guys going to carry guns. That is OK because you did not hire them for that purpose. Not everyone is ready or able to use a firearm safely. I recommend taking the ones that are qualified and using them because you will still need unarmed officers. Your hiring process may need to be tightened a bit more than what we talked about in Chapter 4. It would be negligent to arm security officers that had a violent past, a history of drug use, or certain other criminal history. As for the psychological and other pre-employment screenings you might see in a police department, I would challenge their ability to foresee misconduct. Look at all the issues we have with police officers using excessive force, racial profiling, and badge-heavy attitudes. I am sure these exams help but they do not put me at ease.

I recommend a “working background.” Hire someone to be unarmed. Require that they work six months or so before moving into armed. This gives you a chance to see their demeanor, character, and people skills before giving them a dangerous weapon.

Training

When I started in the business, management would ask you if you had your own gun and if you had any experience carrying one. Are you kidding me? Yes, they did have some crazy stuff happen until finally the city made all security give them up. This lasted a few years, and in a different era, we brought them back…carefully. Training needs to focus on three areas.

1. Weapon Use—This includes some classroom on how guns work, the legality of using deadly force, revisiting arrest and search laws, and private citizen vs. sworn police officer. You also need copious amounts of range training. Proficient use of a firearm must be achieved. Use a certified instructor (NRA is the program with which I am familiar). I suggest using their qualification program instead of coming up with one that has not been tried in court. Do not dumb-down this program just because you have guards instead of cops. Same guns. Same bad guys. Same death and destruction. Many cops shoot bad enough in a stressful situation. Imagine how someone with less training would shoot.

2. Use of Force—This should already be part of your new hire training. You need what you might call an advanced version for your armed officers. The use of deadly force is obviously a serious notion. When it happens, it will likely be unsupervised, uncoached, and without a do-over. Make sure your officers are confident as to when they will draw and/or fire those weapons.
3. Equipment—I am sure every director has their personal favorite and I will not advise you on which guns to use. The only recommendations I have for you are not to let employees use their own guns; and use semi-automatics as opposed to revolvers. I have seen some companies that use wheel guns because they are kind of idiot-proof. Say that out loud. "I am going to give an idiot-proof deadly weapon to my officer." Just go with the fancy pistols and train them how to use them.

Now to complicate things further. If your officers are going to carry guns, what other options will they have for use of a "lesser" force. For example, they encounter a crazy homeless man swinging an umbrella at everyone. Will they be expected to shoot him? These guys need some intermediate weapons to give them non-lethal options. The term less-than-lethal does not do much for me. All weapons are lethal. However, I call them non-lethal because we are not going to train them to use them for deadly force. And we are going to terminate them if they do.

Some options you can consider are Baton, Stun Gun, Taser, pepper spray, mace, and some unusual gadgets that someone might want to sell you. Here are my opinionated summaries of each one. Please do your own research.

Baton—There are three different types of baton or stick. The side handle baton became the best practice for law enforcement in the 1970s. It offers more techniques and options for use. If used correctly, it can be a useful defensive weapon. If used incorrectly, it can do serious damage—especially if used on the head. They also look bad when used. You youngsters look up "Rodney King."

Several police officers were filmed beating on a lone man in Southern California. The beginning of the altercation was not seen by the world, so the perception was that the baton was an offensive, dangerous, and brutal weapon. Not only was the weapon turned into an offensive one, but its excessive use also spawned riots and other injuries.

The "night stick," so named because New York police would carry a longer stick at night, is still used by many police departments. (The short stick is not in use anymore—that I know of—due to its singular offensive purpose.) Even those that sanctioned batons and sticks have largely left those crushers in the car since Tasers came about. There is also an "asp" or collapsible baton. These are metal batons that rapidly telescope into a beating weapon. They are convenient because they can be worn collapsed on the belt but have few defensive purposes.

Before we get to electric stuff, let's look at aerosols and other sprays. Pepper Spray (Oleoresin capsicum) is a mixture of oil and pepper. OC is not lethal, and its effects wear off. Mace is another chemical irritant that is not natural, but its effects are similar and may be more dangerous.

I found pepper foam to be most effective. Some people are resistant to the pepper but that is a small percentage. The problem I have seen with sprays is the overspray or unintentional effects on other people. I am surprised the aerosol still exists as there are other discharge methods that work much better. The stream is more like a squirt gun and shoots the chemical far—beyond knife range. Better yet, is the foam. This stuff comes out more like a shaving cream, yet shoots a fairly small stream of foam a few yards. The foam gets on one's skin and kind of sits there as it burns. Strengths are measured in Scoville Heat Units and you can get a more portent blend than what is sold in mini markets. Get what the police are using.

None of these weapons should be carried without training in their use, effects, and retention. Besides how to use it, the officer needs to learn how to retain it. Especially if they are going to use spray or stick with a firearm, any assault is an attempt at getting the gun, so someone who is fighting for their pepper spray may be fighting for their life.

Tasers

The Taser company drastically changed law enforcement tactics about 30 years ago. There are other stun guns, available widely to everyone, that deliver a shock when placed against the body. The Taser took that concept and made a device that shoots like a gun, but instead of bullets, electric barbs are propelled and deliver the shock from a safe distance. There have been isolated incidents with the use of the Taser that were controversial but not as many as with firearms. Heart failure and other conditions following the use of the Taser were largely due to trauma or pre-existing maladies and not the device itself. Still, perception is reality and anytime one person is adversely affected by a Taser or any other weapon, there will be opposing opinions. I have been shocked by a Taser and used one with a violent assailant and I can say they are effective. I do not endorse any weapon without knowing its intended use, so again I recommend doing your own research and your own risk assessment to see if they are justified for your use.

Weapons Policies

If you are the type that feels segregated from the October 1 shooting in Las Vegas, I understand somewhat. Vegas is different, a little crazy, and this was a one-time deal. I agree with much of that…But…Whether you want to remove it from the important incidents pile, or not, we are on "notice." As you recall from Chapter 1, that means that since we know it *could* happen, we better include it on our risk assessment, so we can prevent it from happening again.

The weapons policy is one of those issues with which just about everyone agrees. Writing it and implementing it are pretty straight-forward. There are some hurdles to consider.

The Law—Yes, unfortunately the law can get in the way of safety sometimes. You need to check with state and local attorneys general and the police to find the exceptions and whether these laws will affect or even be applicable to you. Some jurisdictions interpret the second amendment differently than others.

Private Property—I have not seen a law that compels someone to carry a gun, so that is a good thing for your policy. There are, however, requirements for signs that may be required for your restriction. You can still prohibit guns, but you may have to post certain signs and the statutes.

Signs—You may have the city, county, or state mandating certain signs, so check into that. Otherwise it is private property and you can set whatever policies you want (as long as they are more restrictive and not less restrictive than the laws).

No Exceptions—Oh this will be a fun time: Police are obviously going to be exempt from your policy. Presumably that is on-duty local police officers as part of their official duties. OK, what about traveling police officers? Maybe cops from the next state are staying in your hotel for the purpose of a convention or some sort of class or training. In fact, I have seen many who are traveling on official business such as investigations or transporting prisoners. How will your policy apply to these folks? You can provide them with an exemption and then you will have guys with khaki pants and dark polo shirts with the badge and gun on their hip exposed. Wasn't that the whole purpose of your policy, to get the guns out of sight and out of reach? Take it a step further and they go to the bar after class or to a restaurant and have some wine carrying those exposed weapons. I am pretty sure this is against their department policy and it is probably against ours depending how it goes. I am just raising the questions to think about.

Another potential exception would be the officers from near or far who want to come to your bar or nightclub after work or off hours. If you are doing pat-downs or some sort of weapon search, you are going to have an awkward moment when he or she announces they have a firearm. This of course is a policy you need to work out in advance, but for me it is an easy decision. You do not want weapons in your bar or nightclub carried by anyone. Police officers can get just as drunk as regular folks, can get into fights just like your other customers, and again I am certain that it is against their department policy. Now I am not saying that you have to treat them with kid gloves. You have to work with these people, and embarrassing them in front of their friends and everyone else doesn't do anyone any good. Speaking of problems with police officers in nightclubs, I have found that it is often better to contact the on-duty watch commander to come and resolve an issue of intoxication or violence or a disturbance with a police officer. It can be handled discreetly but professionally in that manner.

Other exceptions to this complicated policy are trade shows, gun shows, hunting expositions, etc. The thing about these events is just about everyone carries a gun, exposed or otherwise. It is better to work out in advance the details of these policies with the event coordinator for the group leader or whomever is going to be enforcing the rules with this particular group.

Do not forget about Mr. Regular Customer. Maybe he spends a lot of room nights in your hotel or attends trade shows. Maybe he is a big game hunter who keeps expensive guns in his room. Will you make exceptions for him? Will you search his luggage? Sound familiar? As we know from a prior incident, nobody should be exempt from this policy. Save the special treatment for food, concerts, and limo rides.

I mentioned before that many of the huge resorts have gone to metal detectors, luggage x-rays, and added personnel just to keep guns out of the hotel. This will be a big decision for you and your executives. Consider your location, clientele, and the ramifications if you do it.

Suppose you say to yourself, "This is too complicated." We never had a problem before. We do not want to rock the boat. This is a great example of foreseeability. Now we have "notice" that bad things with guns can happen. We need to take reasonable steps to prevent it. The idea behind this section is for you to choose these best practices and implement the ones that are called for by your risk assessment.

Conclusion

I think I have imparted everything I know to you now. You know that is not true because the best part about this job is that it changes daily. There is not a day I can remember where I did not want to go to work. I craved the excitement and the problem-solving and the pride of working with my second family. Hopefully, you have a similar interest in your vocation. If not, please find something that gets you going. You will be a better person.

There are just two things I wanted to hammer home one more time.

1. When you make a decision or a plan or solve a problem, always work backward from your objective. This is explained in Chapter 9 in case you forgot.
2. Do not get so comfortable in your position and your practices that you fail to keep up with best practices and innovation. This could make you a liability and cost the company money.

I did not write this book for the money (author is rolling on floor laughing in publisher's office). Frankly, I enjoy writing. I also feel that one learns by teaching and I learned a lot just putting thoughts and memories on paper. Finally, I have a deep respect for our profession and I truly hope you and others carry that torch forward with respect and integrity. Remember the pineapple!

I am delighted to have your feedback. I move around on social media so just search me or try through ASIS or Amazon page.

INDEX

A

Abandoned luggage
  back track, 256–257
  internal procedures, 257
  official response, 257
  risk assessment, 256
Abandoned vehicles, 134, 170
Access control, 13, 22, 25–26, 34, 123, 132, 149, 170–171, 272, 288, 291, 388, 436
Accounting
  charge-offs, 262
  collusion, 261
  credit card fraud, 261–262
  fake vendors, 262
  identity theft, 262
  payroll scams, 260–261
Accounting Department, 260, 262
Accounts Receivable, 262, 370
Across-the-board, 88, 296
Active Shooter, 22, 34, 51, 56, 60, 71, 80, 86, 191, 195–200
Administrative duties, 97, 118
Alarm signal, two-stage, 192
Alcohol
  alcoholic beverages, 298
  awareness, 301
  bar/nightclub, 297
  food service, 364
  intoxicated persons, 298
  minors, 298
  over-pouring, 298
  training, 298
Alcohol Awareness Training, 167
Alcohol Consumption and Crowds, 165
Alcoholic beverages, 20, 297–300
  alcohol, 298–300
  bars, types of, 297
  guest service, 300
"All-hazards" approach, 18
American Express, 262
American Hotel Association (AHA), 39
American Society for Industrial Security (ASIS), 39, 43
  Certified Protection Professional, 280
Americans with Disabilities Act (ADA), 31, 76, 94, 448
Analog cameras, 441
Anger, 379–380
  prevention process, 380
  type A personalities, 379, 380
  type B personalities, 379
Anthrax, 389
Anti-lock brakes, 21
Anti-terrorism, 434–435
Antitheft devices, 353
Aqua Net, 126
Ariana Grande concert, 427
Arm Bar Control, 82
Armed security, 451–460
  contract security, 453
  hiring, 456
  off-duty police, 452–453
  officers, 454
  proprietary security, 454–456
  tasers, 458
  training, 456–458
  weapons policies, 458–460
Arrests, cause injury, 152
Artificial intelligence (AI), 288
Assault on Employee, 10
Assaults in and Around Bars, 341
Assets protection, 65
Atlantic City resort, 145
Attitude, 90
  negativity, 282
  personal growth, 282–283
Audits
  Auditing Department, 258
  control, 265
  guest service, 259
  integrity, 259
  performance, 259
  regulatory, 259
Automatic External Defibrillator (AED), 77, 203, 210

B

Background checks, timing of, 266
Back-of-house, 193
"Backward" method, 112
Bag checks, 311
Bar guns, 336
Bars
  accident, management's obligation/prevent safety
    house, back of, 323
    during night, 323
    patrol around venue, 323
    restrooms, 323
    safety hazards, 323
    safety sweep, 323
  assets, 336
  blood-alcohol content (BAC), 344–345
  CCTV, 348
  characteristics, 340
  CPTED checklist, for venues, 347
  CPTED principles, 343–344
  crowding, 348
  ejection, 325
  entrances/exits, 346, 349
  internal layout, 347–348
  intoxicated persons, 325
  ISO 22341:2021, 342
  ISO 31000, "RISK MANAGEMENT," 342
  nightclub, alcohol, 297
  outdoor drinking areas, 348
  over-charging, 337
    access management, 339
    activity support, 340
    CPTED basic principles, 338
    CPTED concepts, 338
    facility maintenance, 339
    natural surveillance, 339
    order maintenance, 340
    by Russell Kolins, 338
    starting plan, 340–342
    territoriality, 339
  over-pouring, 336–337
  over-serving, 337
  restroom design, 346
  situations/procedures, 322–326
  staff, 349
  training/adherence, 343
  Training for Intervention Procedures (TIPS) program, 344
  trespasses, 325–326
  violence, 324–325
Bartender, difficulty, 337
Basic criminal law, 301
Baton, 457
Beat cops, 119
Bed-and-breakfast, 51
Bed bugs, 215
Behavioral Cues, 344, 345
Behavioral recognition, 321, 350, 359, 370–374
  challenge, 372–374
  objective, 371
  observe, 371
  profiling, 371
  second look, 371–372
  skills, 147
  training programs, 370
Bell Desk, 144, 147, 366
Bellmen, middlemen, 366
Be on the Lookout (BOLOs), 373
Beta site, 289
Beverage server, 323
Bicycle officers, 172
Bike Officers, 156
  control and coordination, 157
  training, 157
Bike patrol policies, 157
B52 lens, 442
Blood-alcohol content (BAC), 344, 345
Blue Campaign, 399
Body language, 231
Bomb dogs, 435
Bomb-resistant glass, 33
Bomb threat, 201
Break policies, 52
Bring Your Own Beer (BYOB), 166
Broken Windows Theory, 171, 339
Brutality, 121
Budgeting, 284
  back-charging, 293
  basics, 284
  benefits, 286
  budget submission, 286
  capital expenses, 287
  defined, 284
  full-time equivalent (FTE), 285

  life safety, 287–288
  lost/found, 293
  overtime, 285–286
  parking, 292
  pitch, 291
  prior year, 284
  process, 284–285
  recurring expenses, 285
  responsibility, 286–287
  restitution, 292
  saving labor, 288–289
  security envy, 289–291
  security revenue, 291–292
  special events, 292–293
  wages, 285
Budget-minded families, 27
Building entry, 184
Business needs, 214
Businesspersons, 165

C

Cadillac Doors, 188
Calamity of errors, 195
Call/email, 276
Call out services, 398
Calls for Service (CFS) reports, 6, 330
Camera patrols, 153, 263
Cameras, 184, 252, 440
  analog, 441
  analog/digital, 441
    analytics, 444
    compression, 442–443
    digital, 441–442
    lens types, 442
    speed, 443
  analytics, in real life, 445
  applications, 444
  in ATMs, 156
  criminal/unsafe activity detection, 446
  detection, 446
  deterrence, 445–446
  elevator camera, 446
  elevators, 446
  in elevators, 160
  facial recognition, 444–445
  for front desk, 156
  investigations, 446–447
  for live investigation, 155
  photograph vehicle license plates, 171
  put up cameras, 445
Candelas, 185
Candlelight, 186
CapEx ROI justification, 288
Capital expenditures, 20
Capital Expenses, 287
Car backfiring, 198
Cardiopulmonary resuscitation (CPR), 30, 74, 79, 101, 210
  instruction, 161
  lecture/workshop classes, 80
  training, 276
Cars, broken window, 134
Cashiers
  coupon, 263
  returns, 263
  voids, 263
Casino accounting departments, 178
Casinos, 25
Casino security, 172, 173
  casino controls, 173–174
  casino patrol, 175–176
  deployment, 177
  detention, 176
  innovation, 177–178
  regulation hierarchy, 175
  security-related issues, 175
  third protection method, 174
Casino security officers, 176
Casino surveillance officers, 178
CAT5/CAT6 cable, 442
Catering/Convention Departments, 292
Catering Department, 375
Celebrities, personal security, 130
Certified bike patrol instructor, 157
Chain of Evidence, 222
Checking ID, on credit transactions, 259
Check-in policies, 399
Check-ins error, 142
Check-printing operation, 136
Chicago E2 Evacuation, 317
Child Protective Services, 408
Chocolates, on guest's pillow, 140
Choke points, 178
Civil law, 37
Civil trials, 236

Clapton, Eric, 204
Classroom training, 67
Claustrophobia, 159, 431
Coat check, 312
Coca Cola, 70
Codes, 38
  Code Adam, 203, 204
  compilation of rules, 42–43
Color
  temperature, 186
  use of, 186
Columbine High School in Colorado, 379
Commercial alarms, 426
Commercial construction, 193
Communication methods, 272, 357
  boss, 272–273
  housekeeper, 358
  maintaining morale, 274–275
  military veterans, 358
  woman walks, 357
  your staff, 273–274
Company manual, 45, 46
Company policies, 301
  hierarchy of rules, 44
  protect assets, 44
Competitive wages, 99–100
Concierge, 147
Confederate Army, 270
Confidentiality, 48, 437
Confidentiality Policy, 48
Conflict of Interest, 48, 401
Conflict resolution training, 382
Confrontational skills, 106
Congress, 204
Contract guard, 104, 105
  security on trial, 104
  witnesses, 104
Contract security, 32, 102, 103, 453
  cost, 103
  proprietary *vs.* contract question, 104
  training/experience, 103
Contract team, 104
Convention centers
  event type, 166
  in-house meeting staff, 165
  institute security, 165
  meeting/exhibition space/kitchen, 164
  risk assessment/security plan, 165
  security needs, 165
Convention Manager, 169
Corona Virus D-19 pandemic, 178, 388, 391
Corona Virus pandemic, 19
Corporate folks, 370
Corporate investigations, 219
Corporate office, 369
Corporate Security, 18
Corruption, 121
Costa Concordia struck, 193
Cost comparison, 288
Cost of living adjustment (COLA), 28, 100
Cost-saving, 289
County Emergency manager, 204
Court-ordered restitution, 238
Co-workers, 60
Crazy Pat, 378
Credit card
  company, 263
  guests, 264
  industry, 355
  victim of, 261
Crime data, 5
  by city, 5
  table, 7
  by zip code, 5
Crime prevention analysis, 181, 243
Crime Prevention Through Environmental Design (CPTED), 25, 114, 180–183
  access restriction, 401
  activity support CPTED principle, 341
  basic principles, 338
  CCTV, 348
  checklist, 347
  crowding, 346, 348
  drinking areas, outdoor, 348
  entrances/exits, 349
  exterior physical security, 182
    landscaping, 183–185
    lighting, 185–187
    physical barriers, 187–188
    walls/fences, 189
  first-generation, 338
  full-scale, 338
  guardianship, 342
  internal layout, 347–348
  internal lighting, 346
  ISO 22341:2021, 340
  Kolins, Russell, 180–182
  lighting, 348

  natural surveillance, 343
  outdoor drinking areas, 346
  physical security, 179, 180
  quality lighting, 345
  restroom design, 346
  second-generation, 338
  staff, 349
Crimes, 38
  analysis, 243
  crime-fighting, 290
  data, *see* crime data
  elements of, 69
  against kids, 276
  triangle, 245, 246
Criminal activity, 4, 6–7, 112, 121, 136, 142, 246, 248, 252, 287, 363, 365, 366–367, 400
Criminal databases, 445
Criminal investigation, 216
Criminal laws, 37
Crisis Management Team, 209
Crowd manager (CM), 166, 168, 306, 431
  training of, 331
C-suite, 219
Culture change
  awareness, 362–363
  communication, 361–362
  ownership, 361
  romantic scandal, 360
  security culture, 359
Culture of safety, 410
Customer service function, 209
Cyanide, 389, 391
Cyber Security toolbox, 179
CyberTipLine averages, 396

D

D.A.R.E program, 120
Data security, 436
  confidentiality, 437
  data investigations, 438
  internal data theft, 437
  internet/email filtering, 437
  passwords, 437
  phishing, 438
  unauthorized hardware, 437
Date of birth (DOB), 305
Deadly Force, 327
Deep pockets category, 420
Defensible Space, 182
Defensive tactics, 81–82, 301
Defibrillators, 79
Defrauding
  elements of, 40–42
  innkeeper, 40
Delegation, irrelevant, 107
Demographics, 166
Department of Homeland Security (DHS), 280
  DHS Bomb Threat Checklist, 201
Department of Justice, 270
Department of Motor Vehicles, 115
Detector wands, 311
Detention, 176
Difficult-to-hire housekeeping positions, 266
Digging deeper, 180
"Dine and dash," 334
Discrimination, 48, 121
Disgruntled employees, prevention of, 196
Dispatch Office, 131
DND signs, 142
Documentation, 51, 83
  liability, 116
  observation reports, 79
Domestic violence, 4, 139, 232, 276, 383, 390, 454
Do-Not-Disturb sign (DND), 19, 136, 137
Door host, 320
Door locks, 33
Door pushers, 141, 249
Draft schedule, 98
Dress code, 321
Drills, 80
Drinking areas, outdoor, 346, 348
Drinking, culture of, 342
Driving Under the Influence (DUI) checkpoints, 303
Drug testing
  cause testing, 256
  post-accident, 255–256
  random, 254–255
Drug transactions, 313
Drug use
  guest-room attendants, 404
  marijuana, 404–405
  parties, 405–406
  sales groups, 406–408
  signs of, 400
  squatters, 408–409

  - sub-letting, 409
  - unplanned parties, 406
- Drunken patrons, 342
- Drunk roll, 266
- Dual controls, 265
- Dual-custody, 149
- *Dumb and Dumber* Movie, 394
- Duty of care, 14
- Duty police officers, 312

E

- EACH restroom, well-documented regular patrol of, 146
- Earthquake, 19, 205
- Education, frontline employees, 391
- Ejections, 315
- Electronic access control, 253
- Electronic key locks, 43
- Elevator meeting, 273
- Email, 53, 230
- Emergency Manager, 276
- Emergency manual
  - hazards/threats, 55–56
  - starting, 56
  - testing, 56
- Emergency medical services (EMS), 200
  - in-custody death syndrome, 81
  - life-threatening condition, 210
- Emergency Medical Technicians (EMTs), 34, 210
  - rural properties, 210
- Emergency phone calls, 132
- Emergency planning, 279
- Emergency procedures, 75, 331
  - active shooter/shots fired, 333
  - earthquake, 332
  - ejections, 331
  - fight, 329–331
  - fire alarm, 332
  - hurricane/blizzard/tornado, 332–333
  - person down, 328
  - power failure, 332
  - smoke/fire, 332
- Emergency response
  - active shooter, 195, 197–198
    - additional details, 200
    - general procedures, 200
    - objective, 199
    - physical, 199
    - police, 199–200
    - security response, 199
  - bomb threat, 201–202
  - earthquake, 205
  - fire, 194–195
  - fire alarm, 192
    - alarm function, 193–194
    - bottom line, 194
    - directional signage, 192–193
    - doors, 193
    - egress, means of, 193
    - false alarms, 194
  - indoor contaminant release, 205–206
  - lost child, 203–204
  - major, 191
  - medical, 202–203
  - outside chemical release, 206
  - panic alarm, 200–201
  - power failure, 205
  - secondary effects
    - casualty incident, 206–208
    - mutual aid, 209
    - recovery, 208–209
  - suicidal, 203
  - weather/blizzards/hurricanes/rain/flood/winds, 204–205
- Employee Assistance Program (EAP), 381, 383, 384
- Employee awareness, 357
  - behavioral recognition, 359
  - communication methods, 357
    - housekeeper, 358
    - military veterans, 358
    - woman walks, 357
  - “human” technology, 359
  - multi-colored search engine, 358
- Employee behavior, 153
- Employee duress, 438–439
- Employee lockers, issuance, 440
- Employee procedures, 50
- Employees
  - non-security, 359
  - point-of-sale locations, 200
  - safety, 333
- Employee theft, 249
- Employee vandalism, 252
- Enforcement Division for the Gaming Control Board, 308
- Enter Physical Security, 182

Entertainment security, 131
Environmentalist, 435
Equal Employment Opportunity Commission (EEOC), 137
Escalators, 158–160
Event type, 166
Executive skills
  associations, 276
  communication, 272
    boss, 272–273
    maintaining morale, 274–275
    your staff, 273–274
  cooperation/collaboration, 270–271
  executive meetings, 271–272
  finding, 269–270
  government meetings, 276
  local trade groups, 276
  mutual aid, 277–278
  networking, 275–276
  nonprofit groups, 276
  online, 277
  public/private groups, 276–277
  regional communication, 277
  regional disaster planning, 279–280
  regional training, 277
  resources, sharing of, 278–279
  written agreement, 278
Exit/re-entry, 321
Eye contact, 90, 115, 133–134, 135, 259, 320, 352, 371, 399

F

Face-to-face policing, 120
Face-to-face supervision, 122
Facial recognition, 433, 445
  casinos, 178
  in hotels, 444
  identify persons, 318
Fact-finding process, 231
Fake IDs, 303
False alarms, 194
FBI report, 71
Federal Emergency Management Agency (FEMA), 33, 280
Federal laws, 41
FedEx, 378
Fictional crime data, 7
Field investigations, 220
Field training, 67
  evaluations, 79
  FTO program, 78
  quality training, 77
  task list, 78–79
Field-training officer (FTO) program, 75, 78
  documentation-centric, 78
  knowledgeable officer, 78
  observation reports, 79
  train trainees, 78
Finder's fee, 87
Fire alarm, 30, 192–194
  alarm function, 193–194
  bottom line, 194
  directional signage, 192–193
  doors, 193
  egress, means of, 193
  false alarms, 194
Firearms training, 73, 453
Fire Command Center, 192, 194
Fire Department inspection, 361
Fire Sprinklers, 192
Fixed posts, 128
  for high-risk areas, 123
Flash Mob, 354
Flood lighting, speaking of, 186
Floor persons, 321–322
  contract officers, 322
  contract security, 322
  dance floor, 322
  restrooms, 322
  secondary exits, 322
Floor watching employees, 335
Food and Beverage Director, 392
Force, use of
  Deadly Force, 327
  policy, 326–328
Foreseeability, 12
Formal Risk Assessment, 1
Free meal complainants, 334
Front Desk, 147, 349
  identity theft, 367
  key theft/room entry, 367–368
  night auditor, 368
  vertical security, 368
Full-time coordinator, 103
Full-time equivalent (FTE), 103, 284, 289
Full-time security officer, 184
Full-time security staff, 201

Funding training
  guest safety, 62–63
  liability, 63
Fusion Center, 277

G

Gaming Control, 175
Gamma hydroxybutyrate (GHB), 313
General manager (GM), 34, 228
Gerrymandering, 5
Get out of here, 198
Global thinking, 108
Going Postal, 378
Golden Rule of Security, 73
"Good ol' boy" system, 173
Gorilla-style security, 299
GPS-equipped phones/devices, 122
Graffiti, 170
Graicunas, V. A., 29
Grand theft auto (GTA), 41
Great Hotel Bathmat Dilemma, 24
Greeters, 115
Greeting, 320
Grooming, 302
Grossly intoxicated persons, 325
Group members, 111
Group thinking, 29
Group, type of, 166
Guards, 115
Guest
  accidents, 239, 243
  behavior, 153
  carelessness, 134
  check-in/check-out date, 241
  error, 249
  interaction, 106
  luggage, 136
  records, 223
  safety, 62–63, 155, 198, 388
  services, 111, 147, 213
  vacation, 213
  witnesses, 239
Guest claims
  statements, 239
  triggers, 239
  witnesses, 239–240
Guest-room, 265
Guest-room attendants (GRAs), 137, 363, 438
  housekeepers, 363
  Stewards, hard-to-hire, 89
Guest-room locks, 447–449
  elevator keys, 449
  latch tool, 448
  smartphone, 447
Guest Service Officers (GSOs), 88
Guest Service Policy, 48
Gun-shot detection, 433
Gym, 406

H

Handcuffing, 44
Handheld magnetometers, 429
"Hands off" policy, 327
Hand stamps, 318
Hand-write, 113
Hand-written-come-down-and-fill-out-this-paper-application process, 89
Harassment, 252
Headwear, 309
Healthcare Information Privacy and Portability Act (HIPPA), 94
Healthcare Patient Portability Act (HPPA)
  interpretation of, 138
  service animals, 138
Health Code, 42
Health Promotion Agency (HPA), 338
Heat sensor, for fire alarm, 15
Heat Sensors, 426
Heat, ventilation, and air-conditioning; boilers (HVAC), 132, 393
"High-class" hotel, 112
High-risk areas, 123
High-risk hotels, 367
High-tech devices, 123
HIPAA (Medical privacy laws), 76
Hiring managers, 106
Hiring officers, 224
Hispanic males, 371
Hospitality, 114
Hospitality industry
  best practices, 43–44
  employees, background checks, 266–267
Hotel/casino, security officers, 116
Hotel investigator, 227
Hotel operator, 367, 368
  credit card, 369

  long distance call, 369
  purchasing scam, 370
  vandalism, 369
Hotels
  admission, 167
  age, 168
  alcohol provision, 166
  banquets, 164
  Bring Your Own Beer (BYOB), 166–167
  convention centers, 164
  crowd management, 168
  demographics, 166
  dress/prohibited items, 168
  event type, 166
  meetings, 164
  merchandise, 167
  minor events, 168
  music, 167
  number of people, 166
  outdoor events, 169–170
  parking, *see* parking
  politics, 167
  security, 141, 167
  security plan, 168–169
  special event permits, 169
  specific group, 166
Hot tubs, 161
Housekeepers, 363–365
Housekeeping, 147
  manager, 241–242
  security, 265–266
House policies
  age requirements, 303
  bottle service, 308
  crowd manager (CM), 306–307
  date drugs, 314
  dress code, 309–310
  drugs, 312–314
  identification, 304–306
  known persons, 307
  prohibited activity, 308
  prohibited items, 310
  searches, 311–312
  tips, 307–308
  VIPs, 307
  weapons, 312
Huge responsibility, 170
Human patrols, 153
Human Resources (HR) Department, 28, 30, 45, 53, 419, 438
Human Security Officers, 119
Human slavery, 397
Humans, speaking of, 288
"Human" technology, 359
Hurricane Irma, 277
Hurricane Katrina, 208

I

ID badges, 440
ID Scanners, 318
ID verification, 301
Imagine working, 207
Improvised explosive devices (IEDs), 434
Inadequate security, 128
Incident action plan (IAP), 33–34, 56–58
Incident overview, 57
Incident Reporting software, 240
Incident response, 209
  bed bugs, 215–216
  crimes, in rooms, 214
  domestic fights, 210–211
  guest-room attendants, 217
  major crime/accident, 216–217
  medical incidents, 210
  proprietary loss/damage, 214
  room disturbance, 215
  room losses, 213–214
  suspicious person, 211
  trespass, 211–213
Industry Standards, 38
Influenza, 392
Informal Risk Assessments, 1
Information Technology (IT), 230
In-house meeting, 165
In-service training
  hiring, 80
  Officer Development Program, 79
"Inside" job, 144
Install access control, 26
Institute security measures, 165
Instructor development training, 67
Insurance company, 455
Integrity checks, 248, 251
Internal crime, 257
  audits
    performing, 259–260

    - types of, 259
  - employee crime stats, 258
    - Auditing Department, 258
    - internal audit, 258
  - fraud detection, 260
  - security audits, 258–259
- Internal data theft, 437
- Internal Risk Assessment, 2
- International CPTED Association (ICA), 181
- International Fire Code, 42, 166, 306
- Internet/email filtering, 437
- Internet protocol (IP), 442
- Interviews
  - objective of, 91
  - witness, 232
- Intoxicated woman, 2
- Investigations, 219
  - analysis
    - data sources, 240–241
    - guest check-in/check-out date, 241
    - metrics, 240
  - bag checks, 253
  - burden of proof, 236
  - character witness, 232
  - cooperation, 235
  - covert cameras, 252
  - crime analysis, 243
    - crime type, 244
    - location, 244
    - sorts, 245
    - suspect, 244
    - time, 244
  - crime triangle
    - location, 246
    - off-property incidents, 246–247
    - reacting to data, 247
    - suspect, 245–246
    - victim, 246
  - criminal, 236–237
  - data analyzing, 241–242
  - drug, *see* drug testing
  - drugs/contraband, 223
  - evidence, 222–223
  - in hospitality industry, 227–228
  - in-house operations
    - integrity checks, 248–249
    - preliminaries, 249–250
    - setup, 250–251
    - sting, 251
    - warnings, 251–252
  - initial response, 220–221
    - preparation, 220
  - interrogation, 234
  - interview, 231
  - non-witnesses, 232
  - outside agencies, 248
  - personnel investigations, 229–231
  - post-interview conference, 233
  - preliminary, 219, 239
  - private *vs.* public, 237
  - purpose of, 220
  - report follow-up, 228–229
  - resignation *vs.* termination, 234–235
  - restitution, 237–238
  - slip/falls, 243
  - starting, 221
    - photos, 221
  - suspect employee, 232–233
  - translators, 236
  - types of, 228, 229
  - undercover operations, 247
  - unions, 235
  - victim, 231–232
  - witnesses, 222, 232
    - interview, 222
  - workers, *see* workers, compensation investigation
- Investigators, 231, 234, 253
  - duties, 219
  - in modern-day Hospitality, 219
- IPhone, 263
- *Iron Man* (movie), 272
- ISIS (Islamic terrorist organization), 360

J

- Jackets, 309
- Jacobs, Jane, 181
- Job
  - description, 30–31
  - full-time, 67
  - market, 86
  - posting, 86–87
- Just doesn't look right (JDLR), 127, 153
  - Doors ajar, 127
  - exits, 127
  - persons, 127
- Justifying security

- arrests/reports, 296
- briefing, pre-shift, 295
- creative scheduling, 294–295
- crime rates, 293–294
- cutting salaries, 294
- guest comfort level, 294
- internal crime, 294
- patrol areas, 296
- procedural changes, 295–296
- spending, 295
- supervisors, 295
- terrorism, 294

K

Key control, 440
Keylocks, 128
Kids
  adult supervision, 408
  owner's manual or hotel guideline, 408
Kolins, Russell, 180, 181, 338

L

Lab/clinic testing, 255
Landscaping
  building entry, 184
  cameras, 184
  music, 185
  outside safety, 184
  parking areas, 184
  patrol, 184
  sight lines, 183
  smoking areas, 185
  standoff area, 183
  walkways, 183
Larceny, 350
Law enforcement, 114
Laws, level of government
  best practices, 38
  codes, 38
  crimes, 38
  industry standards, 38
  "neglect" security, 39
  risk exercise, 39
Leaders
  in management role, 108
  punctuality, 282
Leadership
  creating managers, 106
  delegation, 107–108
  hierarchy, 105
  management, 105
  managing managers, 108–109
  responsibility, 106
  supervision, 106
  training/coaching, 107
LED light, 185
Legionella, 392–393
"Lesser" force, 457
Lethal Force, 75
Liability, 9, 61
License plate recognition (LPR), 171, 450–451
Lifeguard, 160
Life Safety, 287, 288
Light efficiency, 185
Lighting
  backdrop, 187
  because lux/foot-candles, 185–186
  candelas, 185
  color temperature, 186
  color, use of, 186–187
  diffused/shaded lighting, 186
  hotel setting, 187
  internal, 346
  light placement, 186
  photometrics, 185
  shadows, 187
  up-lighting, 187
Light placement, 186
Lockdown and call 911, 198
Locks, electronic key, 43
Logo shirts, 309
"Look the other way" policy, 363
Loss Recovery, 227, 240, 292
Luggage x-rays, 435, 459
Lumens, 185
Lux, 185

M

Managers, 105
  club, 307
  crowd, 306
  general manager, 228
  hiring, 106
  housekeeping, 242
  purchasing, 265

- risk manager, 219
- Manual emergency stops, 161
- Manuals, types of
  - building, 47
  - company manual, 45–46
  - crimes/house policies, 50
  - department policies, 48
  - documentation, 51
  - emergency procedures, 50–51
  - employee policies, 49
  - foreword, 47–48
  - incident response, 51
  - organizational aspects, 48–49
  - policy *vs.* procedure, 44–45
  - posts/patrol areas, 49–50
  - security manual, 46–47
  - systems/procedures, 50
  - training manual, 47
- Manual writing, 51
  - compiling, 54
  - delegation, 53–54
  - other sources, 52–53
  - updates, 54
- Marijuana, 137–138, 404–405
  - laws, 254
  - smoking, in hotel rooms, 405
- Mass exodus, 319
- MasterCard, 262
- Material Safety Data Sheets (MSDS) sheets, 415
- “May I help you,” 368
- “May I help you find something?,” 211
- Medical, 178
- Medical calls, 201
- Medical Response, 221
- Memorandum of Understanding (MOU), 209, 278
- Mental patients assaulting doctors, 377
- Metal detection, 427
- Metal detectors, 459
- Metal Detectors Deployment, 427
- Methylenedioxy-methamphetamine or Extasy (MDMA), 313
- Mexican IDs, 304
- Microsoft Word, 450
- Morale, 111, 120
- Morale maintaining, 110
  - boosters, 112
  - empowerment, 111–112
  - guards, 113
  - image, 112–113
  - proper training/equipment, 113
  - recognition, 113
- Motivation, 111
- Motorized security vehicles, 172
- Motorola radio, 449
- Multi-colored search engine, 358
- Multi-tasking, 131
- Mumbai attacks, 182
- Muscle memory, 60, 73
- Music, 185
- Mutual aid, 209
  - concept of, 277
  - Memorandum of Understanding (MOU), 278

N

- National Center for Missing and Exploited Children (NCMEC), 203, 204, 398
- National Fire Protection Association 730, 341
- National Minimum Drinking Age Act (1984), 303
- National Organization for the Certification of People who Require Wheelchairs, 138
- Nevada casinos, 175
- Nevada Gaming Commission, 173
- Nevada’s dram shop laws, 175
- New York, brutality/corruption/discrimination, 121
- Nightclubs, 145
- Night stick, 457
- 911 operators, 200, 210
- No Colors policy, 40
- “No force”/“hands off” policy, 73
- Noise Complaint, 4, 9
- Non-criminal, 217
- Non-deadly force, 327
- Non-disclosure agreement, 71
- Non-revenue generating department, 284, 288
- Non-risk generating duties, 104
- Non-security employees, 359
- Norovirus, 388, 391–392
- Notice, 414
- No Tolerance policy, 214
- “No Trespassing,” 151
- No victim no crime, 261
- Nuts-and-bolts manual, 56

O

Occupational Safety and Health Administration (OSHA), 22, 377, 382
  OSHA General Duty Clause, 216
  regulations, 410
Off-duty police, 452
Officer, better-trained, 65
Officer Cool, 133
Officer Development Program (ODP), 79, 88, 101, 102
Officers, cross-section of, 111
One Fire Marshall, 316
One-strike rule, 12
Online training, 166
On-the-job training, 301, 395
Open Door Policy, 110
Operations manuals, 50
Organizational skills, 148
Organization needs, 106
Organization of Security Department, 28
Organized retail crime (ORC), 354
Outdoor pool system, 162
Out of sight, 182
Outside safety, 184
Overcrowding, 159
Over-pouring, 298
Over-serving
  door hosts, 337
  intoxication, 337

P

Panic alarms, 154, 200
Parking, 184
  access control, 171
  accomplishes, 172
  authorization, 134
  cleanliness, 170
  garage, 216, 414
  lighting, 171
  parking enforcement, 172
  restrictions, 22
  security patrol, 172
Part of Security Plan, 26
Party-pooper, 364
Passenger behaving, 358
Passive patrol, 145
Passwords, 437
Patrol, 119
  basics, 119
  cooking/unsafe practices, 140
  dispatch, 131
    communication, 132
    documentation, 132
    system monitoring, 132
  domestic fights, 139–140
  door ajar, 140–141
  duties, 135
  eye contact, 135
  greeting, 135
  headcounts, 134
  hotel, 126–127
    combining layers, 128–129
    risk assessment, 128
  housekeeping, 137
  inadequate security, 129
  lobby, 147
  loiterers, 135
  lost/found, 147
    administration, 147–148
    thieves, 148
  marijuana, 137–138
  parking, 134
  parties, in room, 138–139
  patrol procedures, 132–133
  physical protection system
    deployment, 116–117
    people, 114–116
    work force, 117–118
  posts, 123
    elevators, 125–126
    orders, 125
    types, 123–124
  prevention, 119–122
    policing, history of, 120
    two cities, tale of, 120–121
  privacy, 142
  property, 114
  purse advisories, 134–135
  restrooms, 145–147
  room entry, 135–136
  room inventories, 143–144
  room thefts, 144
  safety, 133–134
  security measures, 149
    arresting, 150
    camera placement, 154–156

    - refuse service, 151
    - search stations, 149–150
    - video patrol, 153–154
  - service animals, 138
  - spas/pools
    - chemical hazards, 162
    - hot tubs, 161
    - lifeguard, with property risk manager, 160
    - pool parties, 162
    - pool rules, 160
    - safety equipment, 161
    - theft, 162–163
    - treatments, 161–162
  - special training
    - bike, 156–157
    - escalators, 158–160
  - tracking, 148–149, 439
    - found objects, 148
    - items, disposition of, 149
    - math, 149
    - storage, 148–149
    - valuables/cash, 148
  - trespassing, 151
    - last resort, 152
    - procedures, 152–153
  - underage drinkers, 139
  - unknown guest, 142–143
  - valet, 163
    - employee theft, 164
    - guest accidents/injuries, 164
    - vehicle damage, 164
  - violent crimes, 145
  - VIP protection, 129–131
  - weapons policies, 144
  - welfare check, 141
  - wheelchairs/mobility devices, 138
- Patrol officers, 115, 121
- Patrol schedule, 123
- Patrol techniques, 106
- Patron’s safety, 343
- Payment Card Industry (PCI), 262
- Payment negotiation, 335
- Payroll scams, 260–261
- People factor, 118
- Perfect World, 410, 411
- Personal growth
  - attitude, 282–283
  - respect, 282
  - responsibility, 280
  - stress, 280–281
  - tactical planning, 283
  - time management, 281
    - delegation, 281
    - visibility, 281–282
  - work ethic, 280
- Person down
  - accidents, 328
  - illness, 328
- Personnel files, 230
- Personnel investigation, 236
- Personnel Investigations section, 248
- Phone calls, 94
- Photometrics, 185
- Physical Protection System (PPS), 21, 26, 39, 105, 114, 119, 179–181, 423
  - anti-collision sensors, 21
  - policies and procedures, and technology, 21
- Physical searches, 311
- Physical security
  - personnel, 179
  - policies, 179
  - resources, 180
  - Risk Assessment, 180
- Pinkerton, Allen, 270
- PIN numbers, 156
- Pitch
  - executive summary, 291
  - moral, 291
  - preparing, 291
- Plastic safety signs, 15
- Police
  - departments, 120
    - official training style, 156
  - detective contacts, 136
  - interview, 235
  - negatives of hiring, 452
  - retired police officer, 454
- Policies, “use of force,” 152
- Policy excerpts, 231
- Policy manual, 31
- Policy violations, 44, 121, 156, 234, 236, 238–239, 248–251, 400
- Policy Writing, 105, 365
- Politicians, personal security, 130
- Pool access, to hotel guests, 162
- Pool drain suction, 161
- Pool rules, 160
- Poor grammar, 225

Popular employee scam, 263
Population served, by LAPD, 120
Portman Group, 340
"Position" tracking, 102
Posts
  door host, 320–321
  floor person, 321–322
  line control, 319–320
  setup, 320
Power failure, 56, 159, 205
PowerPoint®, 68
"Pre-con" meeting, 57
Pre-employment testing, 254
Pre-emptive risk assessment, 17
Pre-gamers, 313
Pre-shift briefing, 295
Preventative Patrol, 121–122
Prevention officers, 351
Pre-violent behaviors, 315
Pre-violent indicators, 320
Prior training, 60
Prison guard, 85
"Privacy" section, 142
Privatizing EMTs, 178
Professional security officer, 73
Prohibited items, 320
  coolers, 394
  microwaves/other appliances, 393–394
  pizza coupons, 394
Property, 153
Property theft, 9
Proprietary *vs.* Contract question, 104
Prostitution, 397
  compelling, 401
  criminal enterprise, 354
  nightclub, 308
"Provide security patrol," 26
Psychoactive drugs, 254
Public officials, 271
Public/private partnerships, 280
Pulse nightclub shooting, 452–453
Purchasing Department, 264

Q

Quality, 65–66
Quality out, 65–66
Quarantined area, 428

R

Radio Frequency Identification (RFID) chips, 126
Radios, 449
Radio signal, 441
Randomly patrol, 124, 132
Ready-made signs, 160
REAL ID Act (2005), 304
Reasonable accommodations, 31
"Reasonable person" rule, 364
Reasonable person test, 256
Receiving
  false orders/return thefts, 265
  lost merchandise, 265
  outgoing theft, 264
  receiving theft, 264–265
Receiving management, 265
Recruiter, 86
Recurring expenses, 285
Reduce turnover, 111
Refusing entry, 151
Regular patrol, 124, 128
Reno Air Races, 279
Report writing, 223
  attachments, 226
  corrections, 225–226
  format, 224
  narrative, 224–225
  next steps, 226
  report writing software, 227
  retention, 226–227
Report writing software, 450
Requirements, 87
Reservation center, 368
Restaurants, 263–264
  allergies, 334
  financial stuff
    credit cards, 335–336
    walk-out, 334–335
  food poisoning, 334
  slips/trips/falls, 333–334
Restroom Maintenance Log, 421
Retail
  antitheft devices, 353
  arrests, 351–352
  cameras/mirrors, 353
  catching shoplifters, 350–351
  credit cards, 354–355

  organized retail crime (ORC), 354
  policies, 349–350
  preventing shoplifting, 352
  retail staff training, 352–353
  shoplifting, 350
  store layout, 353
Retail staff training
  clerk patrol, 352
  communication, 352–353
  follow-up, 352
  greeting, 352
Returned to owner (RTO), 148
Revenue-generating departments, 293
Rhode Island Station fire, 316
Ricin, 389
Riding techniques, 157
Risk assessment, 22, 23, 117, 128, 131, 133, 169, 177, 180, 228, 243, 256, 316, 365
  example, 3
  external, 1–2
  foreseeability, 10–11
    managing, 12
  incident data, gathering proprietary, 8
  internal, 2–4
    probability, 4
    property division, 3
    severity, 4
    threats list, 3–4
  likelihood determining, 8–9
  living document, 13–14
  local crime data compiling, 7
  local crime data gathering, 4–6
  managing threats, 17–19
  market incident data, gathering, 8
  media questions, 19
  notice, 11
  police data/statistics, 6–7
  pre-emptive risk assessment, 17
  premises liability, 1
  process, 2
  reaction, 16–17
  reasonable steps, 19–20
  risk management, 13
  security, 15–16, *see* security plan
  and security plan, 165
  software, 2
  step of, 9–10
  talking risk, 14
Risk, assumption of, 14
Risk-gambling, 16
Risk management, 13, 289
Risk Management, Human Resources, and Facilities, 271
Risk manager, 23, 227, 228
Risk Manager/Claims Department, 240
Robots, 451
Roofies, 314
Rookie, The, 133
Room inventories, 143
Rowdy Behavior, 320
Rubbernecking, 350
Rules, hierarchy of, 37
Run, Hide, Fight, 198

S

Safety
  accidents, 419–420
  accountability, 412–413
  awareness, 416
  branding, 414–415
  committee members, 416
  communication, 418
  compliance, 415–416
  coordinator/manager, 412
  culture of, 410–411
  departmental inspections, 417
  documentation, 420
  efficiency, 414
  escalator shutdown, 421–422
  executive team, 411–412
  hazards, 116, 122, 147
  house, back of, 323
  insurance company, 419
  newsletter, 418
  objective, 410
  participation, 413
  program, 415
  restroom logs, 421
  restrooms, 323
  risk management, 420–421
  safety committee, 416–417
  safety newsletter, 418
  safety suggestions, 418–419
  safety sweep, 323
  safety wall, 418
  spill stations, 421

  sweeps, 421
  training, 417–418
  trickle-down feelings of, 62–63
  value, 411
  violations, 252
  workers' compensation, 419
Safety committees, 416
Safety manager, 415
Sales Department, 271
Sanitation program, 392
Sarin, 389
Scary sidewalk, 155
Secret Service, 130
Security
  audit, 258
  culture of, 362
  staff of, 99
  on trial, 99, 104
Security awareness
  criminal activity, 366–367
  and guest service, 363
  housekeeping, 363
    drugs/paraphernalia, 363–364
    parties, 364–365
    weapons, 365
  prostitution, 365
  safety hazards, 365
Security-changing events, 427
Security culture, 359, 433
Security department, 46, 129, 145, 223, 238, 256, 275
  organization of, 28–30
  overall property, 32–33
  policies/procedures, 30–31
  specific areas, 33
Security departments, 47, 76, 87, 177
  organization of, 28–30
Security directors, 22, 266, 269, 272, 275, 280, 281
  hospitality industry, 444
  resourceful, 444
Security Directors Association, 276, 277
  Human Resources Director, 252
Security expert, 269
Security Is Everyone's Job, 363
Security job, 69, 72
Security, layers of, 114
Security/management, call, 368
Security manual, 45, 125
Security measures, 21, 128, 196
  physical, 196
Security needs, 165
Security officers, 51, 56, 110, 174, 176, 199, 211, 258, 265, 274, 373
  deployment of, 177
  needed to intervene, 329
  on patrol, 145
  patrolling, 141
Security plan, 20, 25, 97, 116–117, 128, 149, 150, 168, 170, 365
  accident/incident prevention, 23–24
  building, 24–25
  crime prevention, 21
  crime triangle, 21
  decisions, 24
  outlining, 26–28
  physical protection system (PPS), 21–22
  plan, 22–23
  shotgun method, 24
Security posture, 31, 48
  of property, 114
Security staff, 102, 347
Security systems, 128
Security team, 48
Security technology, 290
Security Theater, 71, 121
Security Vulnerability Assessment, 340
"*See and be seen*," 339
See Something Say Something campaign, 180
Segway, 172
Self-aware, 246
Self-conscious, 226
Self-motivators, 273
Sexual Harassment and Confidentiality, 53
Sexual Harassment Policy, 48
Sexually assault, 128
Sexually harassed, restaurant worker, 230
Shadows, 187
Shift manager, 29
Shooter, unknown, 196
Shoplifting, 350
"Short-handed," 124
"Shotgun" approach, 98, 112, 116
Sight lines, 183
Skynet, 288
Smoke Detector, 426
Smoking areas, 185, 317
Smuggle, 140

Social engineering, 374, 376
  credit card company, 376
  front desk, 374–377
Social media, with bad intentions, 402
Social Security number, 267
Software, report writing, 450
SOP manual, 46
Span of Control (1933), 29
Special security, 130
Specific group, 166
Sprinkler heads, 194
Staffing
  application process, 89–90
  background, 92
    drug testing, 94
    employers, 93–94
  before hiring, 94–95
  deployment, 96
    minimum, 99
    schedules, 97–98
  guards/officers, 85–86
  hiring, 86
  interview, 90
    group, 92
    questions, 91–92
    second, 92
    standard questions, 91
  orientation, types of, 95–96
  recruitment, 86
    job posting, 86–87
    loosen up, 88–89
    qualifications, 87–88
    screener, 87
    starting wage, 88
Standard Operating Procedures (SOPs) manual, 45
Standards, guidelines, 43
Standoff area, 183
Star Trek, Into Darkness (movie), 108
State of Wisconsin Department of Administration, 381
"Sterile" environment, 428
Storage Wars, 366
Storing contraband, 366
Street crime, 247
Stuck elevator, 159
Supervisors
  managers, 105, 115
  trainee, 101
Surveillance, 339
Surveillance officers, use patrol routes for cameras, 153
Surveillance watches, 174
Suspicious Activity, 122
Swab tests, 255

T

Teach GRAs, 365
Technical duties, 106
Technological advancements, 114
Technology
  artificial intelligence, 433
  crowd management, 430–433
    communication, 432
    direction, 432–433
    planning, 431–432
  fire alarms
    alarms, types of, 426
    communicator, 426
    fire sprinklers, 426
    panel, 425
    sensors, 425
  guest surveys, 423
    employee development, 424
    fresh ideas, 425
    guest satisfaction, 424
    liability, 425
  gun shot detection, 433
  metal detectors, 426
    bottles/liquor, 428
    cell phones, 430
    concerts, 427
    manpower, 430
    placement, 428
    policy, 427–428
    searches, 428–429
    settings, 428
    smoking/re-entry in and out, 429–430
    wands, 429
Terrorism, 366–367
Theft
  auto data, 9
  internal, 260
  from lockers, 162
  from rooms, 140
Thinker, The, 133
Threat Assessment (TA), 17, 19

Threat Assessment Teams (TATs), 383
Threats
  bar/club, 316
  listing, 3
  man-made, 55–56
  natural, 55
  probability of, 9
  risk of, 10
  severity of, 4
Three Strikes Rule, 138
Time-consuming process, 224
Timing, 290
  speaking of, 290
  "timing is everything," 109
"Tough Guy" approach, 320
Tour tracking, 439
Toxic air, 205
Tracking information, 148
Traffic accident, 6
Traffickers, 402
Trafficking/prostitution, 397
  child pornography, 402–403
  child sex trafficking, 402
  end-user, 397
  front desk clerks, 399–400
  guest-room attendants, 400
  hotel room, 396
  online enticement, 402
  pimp, 397–399
  prostitution glossary, 403–404
  solutions, 399
  trick roll, 395
  valet/bell/concierge, 400–402
  victimless crime, 394
Trainee, supervisor, 101
Training
  ability, 59–60
  appearance, 301–302
  for bike officers, 157
  consistency, 60–61
  Crowd Manager, 331
  culture, *see* training culture
  equipment, 457
  exercise, 80
  and experience, 103
  firearms, 73
  funding, *see* funding training
  inadequate/negligent, 62
  in-service, 79, 80
  liability, 61–62
  manager's job, 107
  non-trainable skill, 95
  qualified instructor, use of, 81
  quality, 77
  repair procedures, 157
  shared labor, 302–303
  topics, 301
  use of force, 457
  weapon use, 456
Training culture, 63
  end of time, 65
  everyone, 64–65
  manager, 64
  new guy, 64
  security department, 64
  unique classes, 64
Training for Intervention Procedures (TIPS) program, 344
  On-Premises program, 344
Training manager, 64, 67
Training manual, 47
Training officer, 96
Training program, 67, 111
  basic laws, 69
  classroom, 67–68
  company policies, 75
  emergency procedures, 75–76
  force, use of, 70–73
    intermediate weapons, 74
    lethal force, 75
    physical presence, 73–74
    "soft"/"empty" hand controls, 74
    verbal commands, 74
  guest service, 76–77
  hands-off, 71
  laws of arrest, 69–70
  necessary, 72
  reasonably necessary, 72
  report writing, 75
  search/seizure, 70
  security theater, 71
  training components, 67
  training objective, 68–69
  word-of-mouth, 61
Train security officers, 257
Train trainees, 78
Transportation Security Administration (TSA), 432

“Trespass,” 151, 212, 325–326
Trick roll, 395
Troublemakers/criminals, 151
Truth-telling style, 233

U

Unauthorized hardware, 437
Under-the-table, 267
United States
  public/private partnerships, 280
  United States Postal Service (USPS), 378
Unknown shooter, 196
Unwritten rules, 47
Up-lighting, 186
Urine testing, 255
Use of Force, 32, 61, 73, 74, 326
UV test, 306

V

Valet claim ticket, 163
Valet parking
  background check, 385
  claims/incidents, 384–385
  clearance, 386
  concourse, 387
  controversial trick, 385
  drunk drivers, 386–387
  height, 386
  keys, 387–388
  office, 387
  podium, 387
  point, 387
  porte-cochère, 387
  reducing obstacles, 385
  theft claims, 386
  ticket, 386
  video cameras, 385
Valve controlling, 162
Vehicle Borne Senior Citizen Device, 188
Verbal Commands, 74
Verbal translations, 230
VHS tape, 443
Victims, 398
  first, 231
  shooter awareness training, 60
Video
  analytics, 291, 433, 444
  coverage, 154
  missing, 228
  patrol, 153
  recording, 252
  review, 224
Video system, 440
  real-time images, 450
  recorders, 443
  surveillance cameras, 338
  surveillance system, 440
Violence, 314, 324
  arguments, 324
  body language, 325
  closing duties, 319
  from criminal acts, 377
  domestic, 9
  ejections, 315–316
  emergency exits, 317
  hand stamps, 318
  ID scanners, 318
  intoxication, 325
  occupancy, 316
  pre-violence, 315
  pre-violent indicators, 324
  re-entry, 317–318
  restrooms, 317
  staffing ratios, 316–317
  taking action, 315
  Type II, 377, 378
  Type III Workplace Violence, 383
  Type IV, 383
  yelling, 324
Violent behavior, 309
Violent crime, 11
VIP guest, 171
Virginia Tech classroom, 198
Virtual matrix, 442
Virus
  airborne, 389–390
  contact poisons, 390
  Corona Virus D-19 pandemic, 388
  guest safety and security, 388
  ingested poisons, 390
  mitigation, 391
  Norovirus, 388, 391–392
    preventing, 392
  overview, 389
  prevention, 390–391

  water supply, 392–393
Visa, 262
Voter ID card, foreign, 304

W

Wages, 285, 286
  competitive, 99
  entry-level, 101
  increment, 101
Wage structure
  base wage, 99–100
  benefits, 100
  experience, 100
  officer development program (ODP), 101–102
  raises, 100
  reputation, 100–101
  survey, 99
  training, 100
Walkways, 183
Waste, 116
  housekeepers, 363
  of resources, 155
Weaponize, 451
Weapons, 382
  intermediate, 74
  policies, 144, 458–460
Web filters, 438
Weingarten Act, The, 235
Welfare check, 141
"Wet floor" signs, 15
Wi-Fi, to phone, 449
Wilde, Oscar, 85
Witness interviews, 232
Witness statement, 228
Woman, intoxication, 2
Workers
  better-trained, 65
  compensation, 32, 419
  compensation investigation, 238
Workers' Compensation Department, 238
Workforce-management, 57
Workforce-posts, 57
Workplace violence policy, 196
  anger, 379–380
  conclusions, 379
  criminal acts, 377
  customer/client/patient violence, 377
  developing program, 380–382
  domestic violence, 383–384
  history, 378–379
  prevention of, 380
  related policies, 382
  threat assessment teams (TATs), 383
  training program, 382–383
  violence stemming, from personal relationship, 378
  worker-on-worker violence, 378
Workplace Violence section, 197
World Trade Center, 18

X

X-ray machines, 368, 435
  airport-style, 367
  for luggage, 435
  portable, 368

Z

Zero tolerance, 94, 309, 330, 380
Zipper plastic bags, 222